Steve D. Larson, OSB No. 863540
Email: slarson@stollberne.com
Jennifer S. Wagner, OSB No. 024470
Email: jwagner@stollberne.com
STOLL STOLL BERNE LOKTING & SHLACHTER P.C.
209 SW Oak Street, Suite 500
Portland, OR 97204
Telephone: (503) 227-1600

Attorneys for Plaintiffs

[Additional Counsel Listed on Signature Page.]

UNITED STATES DISTRICT COURT

DISTRICT OF OREGON

PORTLAND DIVISION

JAMES SIMMS; ERIC MILLER; MICHAEL DILLON; CARTER WILSON; JIMAYA GOMEZ; LORI HOWICK; EUGENE CORDERRE; DELMITA BOYKINS; LINDA PHILLIPS; HARLEY ODA; KENNETH WOOLSEY; JUSTIN WHIPPO; GERALD WILKIE; DAVID COPELAND; JEFFREY CROWN; RICHARD BASHAM; HOWARD KRAMER; MARTA BOLANOS; GERALD MARK TRUBEY; KEITH ALLEN CHICK; RYAN CLARKE; KRISTINA MORIN-NIEVES; ANDREW MONTOYA; RICK SNYDER; SARAH STONE; ZACHARY RICHARD; ASHLEY PRICE; JOHN NACCI; KATHLEEN GREER; VERONICA GARDNER; JERRY PEACOCK; MATTHEW FICARELLI; JESSICA GROSSKOPF; HIBBITS INSURANCE, INC.; DK SYSTEMS, LLC; and INTELLIGENT TECHNOLOGY INTEGRATION SOLUTION, LLC; individually and on behalf of all others similarly situated,

Plaintiffs,

vs.

INTEL CORPORATION,

Defendant.

Case No. 3:18-cv-01567

CLASS ACTION ALLEGATION COMPLAINT

<u>DEMAND FOR JURY TRIAL</u>

Plaintiffs, individually and on behalf of the members of the Class defined below, allege the following against Intel Corporation ("Intel"), based upon personal knowledge with respect to themselves and on information and belief derived from, among other things, the investigation of counsel and review of public documents as to all other matters.

INTRODUCTION

1. In January 2018, it was publicly revealed for the first time that Defendant Intel's processors (also known as chips or central processing units ("CPUs" or "processors")), have significant security vulnerabilities. A CPU is the "brain" in every computer and mobile device and processes all of the essential applications, including the handling of confidential information such as passwords and encryption keys. Maintaining the security of confidential information is a fundamental function of all CPUs.

2. The attacks identified in 2018, dubbed "Meltdown," "Spectre," and "Foreshadow," exploited defects in Intel's CPU design. More specifically, when Intel's processors engaged in speculative execution, the processors made information, which should have remained secure and inaccessible to unauthorized use, accessible in the processors' unsecured cache subsystem. In so doing, Intel's processors created a vast security vulnerability that could be accessed through a number of different exploits (the "Defect(s)").

3. The Defects that allow these attacks are the direct result of Intel's knowing decision to sacrifice security in favor of speed in its ongoing competition with rivals such as AMD. Moreover, Intel's decision to forego security for the sake of speed was contrary to the public statements it made about the security of its processors.

4. While Intel has yet to come forth with a full and candid description of all facts known only to it concerning the unprecedented security Defect, what Intel has admitted is

damning. Intel's flawed processor design affects the x86-64x core processors CPUs Intel manufactured in the last 20 years ("Intel's CPU(s)"). Specifically, in its push for speed, Intel designed its CPUs to utilize certain techniques, such as speculative execution and out-of-order execution, in a manner that left users' confidential information exposed and vulnerable to unauthorized access by third parties. Since Meltdown and Spectre became public, researchers and academics have described other means of unauthorized access, including Foreshadow in August 2018, that exploit Intel's flawed CPU design.

5. In a nutshell, speculative execution allows a CPU to run instructions from software programs or applications, before knowing whether an instruction is required or whether access to information is authorized. Intel's defective implementation of "speculative execution" maintains accessed user information, including confidential information, within fast memory on its CPUs ("cache") in a vulnerable manner, and thus exposes user data to substantial security risk by unauthorized third parties.

6. Meltdown, Foreshadow, and Spectre are part of a class of attacks called side-channel attacks that allow unauthorized third parties to exploit Intel's processor vulnerabilities to gain access to confidential information.

7. Unbeknownst to the consuming public, Intel has known for several years that its CPU design, which permitted unauthorized memory access during speculative execution, could be exploited by side-channel attacks. Further, Intel has been aware of various methods that would secure its CPUs and failed to implement them. Indeed, AMD has reported that its processors are not affected by either Meltdown or Foreshadow.

8. As a leader in the global CPU industry, Intel knows the critical importance of both performance and protecting consumers' sensitive data from unauthorized access. Intel also knows

the multitude of harms that foreseeably flow to individual consumers when sensitive data is stolen by criminals, including, among other things, identify theft, fraud, credit and reputational harm, erroneous tax claims, and extortion. Indeed, Intel's success is largely based on the advertised speed and security of its CPUs.

9. While some patches have become available to address Meltdown, Foreshadow and Spectre, they are inadequate and materially affect the performance of Intel's CPUs. The only true fix would be to exchange each defective CPU for a device containing a processor not subject to the security and performance Defect.

10. Incredibly, even after Intel learned of the security Defect, it unreasonably delayed disclosing the vulnerability for months, thereby increasing exposure, risk, and injury to Plaintiffs and the other class members. During this delay and before the Defect was made public (and patches made available), former Intel CEO Brian Krzanich exercised and sold off nearly 900,000 company shares and stock options—making about $24,000,000.00—months after being informed of the significant security vulnerability in its flagship CPUs but before Intel publicly disclosed the problem. The stock sale left Krzanich with just 250,000 shares of Intel stock—the minimum that he is required to own under his Intel employment agreement. By withholding the facts concerning the defective CPUs, Intel put its own interests ahead of the very consumers who placed their trust and confidence in Intel and benefitted itself to the detriment of Plaintiffs and Class members.

11. Intel's actions and omissions violate the well-established legal and statutory duties it owed to Plaintiffs and the class members. Plaintiffs allege claims for, among other things, fraud, breach of the implied warranty of merchantability, unjust enrichment, and violations of the consumer protection statutes of various states and seek, on behalf of themselves and the Classes

defined herein, damages (both statutory and punitive), restitution, and declaratory and injunctive relief.

JURISDICTION AND VENUE

12. This Consolidated Complaint is intended to serve as a superseding complaint as to all other complaints consolidated in this multidistrict litigation and shall serve for all purposes as the operative pleading for the Class defined below. As set forth herein, this Court has general jurisdiction over Intel and original jurisdiction over Plaintiffs' claims.

13. This Court has subject-matter jurisdiction pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d)(2), because this is a class action in which the matter in controversy exceeds the sum of $5,000,000, and Intel is a citizen of a State different from that of at least one Class member.

14. Venue is proper in this District pursuant to 28 U.S.C. § 1407 and the April 5, 2018 Transfer Order of the Judicial Panel on Multidistrict Litigation in MDL 2828 or, in the alternative, pursuant to 28 U.S.C. § 1391 because Intel transacts business and may be found in this District.

NAMED PLAINTIFFS

15. **Plaintiff James Simms** is a resident and citizen of the State of Alabama. In or about April/May 2018, Plaintiff bought a new Dell laptop containing an Intel CPU. Plaintiff's laptop receives automatic updates that include the patches released to date. Plaintiff expected the processor to function as Intel advertised and represented and to adequately secure stored data from exploits. Had Plaintiff known that in designing the CPU, Intel failed to take adequate measures to secure stored data, that it would not sufficiently monitor the security of its product, or that certain patches needed to address such security failures would result in the CPU's reduced performance, Plaintiff would not have bought the Dell laptop, or would have paid less for it.

16. **Plaintiff Eric Miller** is a resident and citizen of the State of Alabama. In or about February 2016, Plaintiff bought a new HP laptop containing an Intel 17-6500u @ 2.50 GHz processor; in or about September 2016 an Intel CPU i7-6700k @ 4 GHz and in or about September 2017 an Intel CPU i7-7820x @ 3.6 GHz boost 4.3 GHz. Plaintiff's HP laptop and computers built with the Intel processors all receive automatic updates that include the patches released to date. Plaintiff expected the processors to function as Intel advertised and represented and to adequately secure stored data from exploits. Had Plaintiff known that in designing the CPU, Intel failed to take adequate measures to secure stored data, that it would not sufficiently monitor the security of its product, or that certain patches needed to address such security failures would result in the CPU's reduced performance, Plaintiff would not have bought the HP laptop and Intel processors, or would have paid less for them.

17. **Plaintiff Michael Dillon** is a resident and citizen of the State of Arizona. In or about August 2016, Plaintiff bought a new Acer Aspire laptop containing an Intel Core i7 6500u CPU. Plaintiff's laptop receives automatic updates that include the patches released to date. Plaintiff expected the processor to function as Intel advertised and represented and to adequately secure stored data from exploits. Had Plaintiff known that in designing the CPU, Intel failed to take adequate measures to secure stored data, that it would not sufficiently monitor the security of its product, or that certain patches needed to address such security failures would result in the CPU's reduced performance, Plaintiff would not have bought the Acer laptop, or would have paid less for it.

18. **Plaintiff Carter Wilson** is a resident and citizen of the State of Arizona. In or about December 2012, Plaintiff bought a new HP Pavilion computer containing an Intel Core i5 2400 CPU. In or about October 2013, Plaintiff purchased two different model HP laptops, both

containing Intel Core i7 4700MQ CPUs. Plaintiff's laptops receive automatic updates that include the patches released to date, and it is his practice to install any updates he receives pop up notices about promptly. Plaintiff expected the processors to function as Intel advertised and represented and to adequately secure stored data from exploits. Had Plaintiff known that in designing its CPUs, Intel failed to take adequate measures to secure stored data, that it would not sufficiently monitor the security of its products, or that certain patches needed to address such security failures would result in the CPUs' reduced performance, Plaintiff would not have bought the HP laptops, or would have paid less for each of them.

19. **Plaintiff Jimaya Gomez** is a resident and citizen of the State of Arizona. In or about January 2016, Plaintiff bought a new Apple MacBook Pro containing an Intel Core i7 CPU. Plaintiff's MacBook displays alerts when an update is available, and it is her practice to promptly install updates upon seeing any pop up. Plaintiff's MacBook is up to date, including the patches released to date. Plaintiff expected the processor to function as Intel advertised and represented and to adequately secure stored data from exploits. Had Plaintiff known that in designing the CPU, Intel failed to take adequate measures to secure stored data, that it would not sufficiently monitor the security of its product, or that certain patches needed to address such security failures would result in the CPU's reduced performance, Plaintiff would not have bought the MacBook, or would have paid less for it.

20. **Plaintiff Intelligent Technology Integration Solution, LLC** ("ITIS") is a limited liability company organized under the laws of Delaware and with its principal place of business in California and provides IT services to clients. During the class period, ITIS purchased a large number of products containing defective Intel processors, including but not limited to i3, i5, i7, Celeron, Pentium, Atom and Xeon processors. Following the disclosure of the Meltdown and

Spectre security defects, ITIS installed on its own devices upgrades and patches intended to mitigate those security defects. ITIS expected the processors to function as represented or advertised and to adequately secure stored data from exploits. Had ITIS known that in designing the CPUs, Intel failed to take adequate measures to prevent unauthorized access to stored data, that it would not sufficiently test and monitor the security of its products, or that certain patches needed to address such security failures would result in the CPUs' reduced performance, ITIS would not have bought devices with defective Intel CPUs, or would have paid or sought to pay less for them.

21. **Plaintiff Lori Howick** is a resident and citizen of the State of Connecticut. In or about October 2014, Plaintiff bought a new HP laptop containing an Intel CPU. Plaintiff's laptop receives automatic updates that included the patches released through July 20, 2018, the date the laptop ceased turning on. Plaintiff expected the processor to function as Intel advertised and represented and to adequately secure stored data from exploits. Had Plaintiff known that in designing the CPU, Intel failed to take adequate measures to secure stored data, that it would not sufficiently monitor the security of its product, or that certain patches needed to address such security failures would result in the CPU's reduced performance, Plaintiff would not have bought the HP laptop, or would have paid less for it.

22. **Plaintiff Eugene Coderre** is a resident and citizen of the State of Connecticut. In or about December 2013, Plaintiff bought a new HP Pavilion P7-1415 containing an Intel Core i5 3450 CPU @ 3.10Ghz. Plaintiff's HP Pavilion P7-1415 receives automatic updates that include the patches released to date. Plaintiff expected the processor to function as Intel advertised and represented and to adequately secure stored data from exploits. Had Plaintiff known that in designing the CPU, Intel failed to take adequate measures to secure stored data, that it would not sufficiently monitor the security of its product, or that certain patches needed to address such

security failures would result in the CPU's reduced performance, Plaintiff would not have bought the HP Pavilion P7-1415, or would have paid less for it.

23. **Plaintiff Delmita Boykins** is a resident and citizen of the District of Columbia. In or about August 2011, Plaintiff bought a new Acer Aspire laptop containing an Intel Atom 2600 CPU. Plaintiff's laptop alerts her when new updates are available, and it is her practice to promptly install those updates, usually within days. Plaintiff's laptop is up to date, including the patches released to date. Plaintiff expected the processor to function as Intel advertised and represented and to adequately secure stored data from exploits. Had Plaintiff known that in designing the CPU, Intel failed to take adequate measures to secure stored data, that it would not sufficiently monitor the security of its product, or that certain patches needed to address such security failures would result in the CPU's reduced performance, Plaintiff would not have bought the Acer laptop, or would have paid less for it.

24. **Plaintiff Linda Phillips** is a resident and citizen of the District of Columbia. In or about March 2017, Plaintiff bought a new HP laptop containing an Intel Core i3 5005u CPU. Plaintiff's laptop receives automatic updates that include the patches released to date. Plaintiff expected the processor to function as Intel advertised and represented and to adequately secure stored data from exploits. Had Plaintiff known that in designing the CPU, Intel failed to take adequate measures to secure stored data, that it would not sufficiently monitor the security of its product, or that certain patches needed to address such security failures would result in the CPU's reduced performance, Plaintiff would not have bought the HP laptop, or would have paid less for it.

25. **Plaintiff Harley Oda** is a resident and citizen of the State of Hawaii. In or about 2013-2015, Plaintiff bought a new Intel Core i7 CPU as a component part for a custom build.

Plaintiff's computer containing the i7 processor receives automatic updates that include the patches released to date, and it is Plaintiff's practice to swiftly install any updates when prompted by the operating system. Plaintiff expected the processor to function as Intel advertised and represented and to adequately secure stored data from exploits. Had Plaintiff known that in designing the CPU, Intel failed to take adequate measures to secure stored data, that it would not sufficiently monitor the security of its product, or that certain patches needed to address such security failures would result in the CPU's reduced performance, Plaintiff would not have bought the i7 processor, or would have paid less for it.

26. **Plaintiff Kenneth Woolsey** is a resident and citizen of the State of Idaho. In or about November 2017, Plaintiff bought a new Dell XPS 8930 desktop computer containing an Intel Core i7 8700 CPU @ 3.20 GHz 3.19 GHz processor. Plaintiff's Dell receives automatic updates that include the patches released to date. Plaintiff expected the processor to function as advertised and to adequately secure stored data from exploits. Had Plaintiff known that in designing the CPU, Intel failed to take adequate measures to secure stored data, that it would not sufficiently monitor the security of its product, or that certain patches needed to address such security failures would result in the CPU's reduced performance, Plaintiff would not have bought the Dell XPS 8930, or would have paid less for it.

27. **Plaintiff Justin Whippo** is a resident and citizen of the State of Illinois. In or about July 2014, Plaintiff bought a new Asus laptop containing an Intel Pentium CPU 2117u @ 1.80GHz, 1800 MHz. Plaintiff's laptop receives automatic updates that include the patches released to date. Plaintiff expected the processor to function as Intel advertised and represented and to adequately secure stored data from exploits. Had Plaintiff known that in designing the CPU, Intel failed to take adequate measures to secure stored data, that it would not sufficiently monitor the security of

its product, or that certain patches needed to address such security failures would result in the CPU's reduced performance, Plaintiff would not have bought the Asus laptop, or would have paid less for it.

28. **Plaintiff Gerald Wilkie** is a resident and citizen of the State of Iowa. In or about 2010, Plaintiff bought a new Dell laptop containing an Intel Atom N270 processor. Plaintiff's laptop receives automatic updates that include the patches released to date. Plaintiff expected the processor to function as Intel advertised and represented and to adequately secure stored data from exploits. Had Plaintiff known that in designing the CPU, Intel failed to take adequate measures to secure stored data, that it would not sufficiently monitor the security of its product, or that certain patches needed to address such security failures would result in the CPU's reduced performance, Plaintiff would not have bought the Dell laptop, or would have paid less for it.

29. **Plaintiff David Copeland** is a resident and citizen of the State of Iowa. In or about November 2016, Plaintiff bought a new Inspiron laptop 7000 series containing an Intel i7 6500U CPU @ 2.5 GHz. Plaintiff's Inspiron laptop receives automatic updates that include the patches released to date. Plaintiff expected the processor to function as Intel advertised and represented and to adequately secure stored data from exploits. Had Plaintiff known that in designing the CPU, Intel failed to take adequate measures to secure stored data, that it would not sufficiently monitor the security of its product, or that certain patches needed to address such security failures would result in the CPU's reduced performance, Plaintiff would not have bought the Inspiron laptop, or would have paid less for it.

30. **Plaintiff Jeffrey Crown** is a resident and citizen of the State of Kansas. In or about September 2015, Plaintiff bought two new Intel Core i7 4790k CPUs. Plaintiff's custom-built computers containing these CPUs receive automatic updates that include the patches released to

date. Plaintiff expected the processors to function as Intel advertised and represented and to adequately secure stored data from exploits. Had Plaintiff known that in designing its CPUs, Intel failed to take adequate measures to secure stored data, that it would not sufficiently monitor the security of its products, or that certain patches needed to address such security failures would result in the CPUs' reduced performance, Plaintiff would not have bought the Intel CPUs, or would have paid less for each of them.

31. **Plaintiff Richard Basham** is a resident and citizen of the State of Kansas. In or about March 2015, Plaintiff bought a new Toshiba laptop containing an Intel Core i7 4700MQ CPU. Plaintiff's laptop receives automatic updates that include the patches released to date. Plaintiff expected the processor to function as Intel advertised and represented and to adequately secure stored data from exploits. Had Plaintiff known that in designing the CPU, Intel failed to take adequate measures to secure stored data, that it would not sufficiently monitor the security of its product, or that certain patches needed to address such security failures would result in the CPU's reduced performance, Plaintiff would not have bought the Toshiba laptop, or would have paid less for it.

32. **Plaintiff Howard Kramer** is a resident and citizen of the Commonwealth of Massachusetts. In or about 2013 or 2014, Plaintiff bought a new Dell desktop containing an Intel Core i3 3240 CPU. Plaintiff's desktop receives automatic updates that include the patches released to date. Plaintiff expected the processor to function as Intel advertised and represented and to adequately secure stored data from exploits. Had Plaintiff known that in designing the CPU, Intel failed to take adequate measures to secure stored data, that it would not sufficiently monitor the security of its product, or that certain patches needed to address such security failures would result

in the CPU's reduced performance, Plaintiff would not have bought the Dell desktop, or would have paid less for it.

33. **Plaintiff Marta Bolanos** is a resident and citizen of the State of Nebraska. In or about 2014, Plaintiff bought a new Samsung computer containing an Intel Core i3 3227U CPU. Plaintiff's computer receives automatic updates that include the patches released to date. Plaintiff expected the processor to function as Intel advertised and represented and to adequately secure stored data from exploits. Had Plaintiff known that in designing the CPU, Intel failed to take adequate measures to secure stored data, that it would not sufficiently monitor the security of its product, or that certain patches needed to address such security failures would result in the CPU's reduced performance, Plaintiff would not have bought the computer, or would have paid less for it.

34. **Plaintiff Gerald Mark Trubey** is a resident and citizen of the State of New Hampshire. In or about November 2014, Plaintiff bought a new Toshiba Satellite C55 laptop containing an Intel N3530 @ 2.16 GHz. Plaintiff's Toshiba laptop receives automatic updates that include the patches released to date. Plaintiff expected the processor to function as Intel advertised and represented and to adequately secure stored data from exploits. Had Plaintiff known that in designing the CPU, Intel failed to take adequate measures to secure stored data, that it would not sufficiently monitor the security of its product, or that certain patches needed to address such security failures would result in the CPU's reduced performance, Plaintiff would not have bought the Toshiba laptop, or would have paid less for it.

35. **Plaintiff Keith Allen Chick** is a resident and citizen of the State of New Hampshire. In May 2015, Plaintiff bought a new Lenovo Idea Centre K450e containing an Intel i7-4790 CPU @ 3.60Ghz – 3.60Ghz. Immediately the Plaintiff's Lenovo Idea Centre K450e had

constant crashes that forced Lenovo tech specialists to eventually replace the processor and motherboard. In March/April of 2018 Plaintiff started noticing a decrease performance, and in August of 2018 another noticeable decrease in performance. Plaintiff's Lenovo computer receives automatic updates that include the patches released to date. Plaintiff expected the processor to function as advertised and to adequately secure stored data from exploits. Had Plaintiff known that in designing the CPU, Intel failed to take adequate measures to secure stored data, that it would not sufficiently monitor the security of its product, or that certain patches needed to address such security failures would result in the CPU's reduced performance, Plaintiff would not have bought the Lenovo Idea Centre K450e.

36. **Plaintiff Ryan Clarke** is a resident and citizen of the State of New Jersey. In or about August 2017, Plaintiff bought a new Apple MacBook Pro containing an Intel CPU. Plaintiff's MacBook receives automatic updates that include the patches released to date. Plaintiff expected the processor to function as Intel advertised and represented and to adequately secure stored data from exploits. Had Plaintiff known that in designing the CPU, Intel failed to take adequate measures to secure stored data, that it would not sufficiently monitor the security of its product, or that certain patches needed to address such security failures would result in the CPU's reduced performance, Plaintiff would not have bought the MacBook, or would have paid less for it.

37. **Plaintiff Kristina Morin-Nieves** is a resident and citizen of the State of New Jersey. In or about January 2017, Plaintiff bought a new HP laptop containing an Intel Celeron N3050 processor. Plaintiff's laptop receives automatic updates that include the patches released to date. Plaintiff expected the processor to function as Intel advertised and represented and to adequately secure stored data from exploits. Had Plaintiff known that in designing the CPU, Intel

failed to take adequate measures to secure stored data, that it would not sufficiently monitor the security of its product, or that certain patches needed to address such security failures would result in the CPU's reduced performance, Plaintiff would not have bought the HP laptop, or would have paid less for it.

38. **Plaintiff Andrew Montoya** is a resident and citizen of the State of New Mexico. In or about December 2017, Plaintiff bought a new Apple Mac Mini containing an Intel Core i3 CPU. Plaintiff's Mac Mini receives automatic updates that include the patches released to date. Plaintiff expected the processor to function as Intel advertised and represented and to adequately secure stored data from exploits. Had Plaintiff known that in designing the CPU, Intel failed to take adequate measures to secure stored data, that it would not sufficiently monitor the security of its product, or that certain patches needed to address such security failures would result in the CPU's reduced performance, Plaintiff would not have bought the Mac Mini, or would have paid less for it.

39. **Plaintiff Rick Snyder** is a resident and citizen of the State of North Dakota. In or about 2016, Plaintiff bought a new Acer laptop containing an Intel CPU. Plaintiff's laptop receives automatic updates that include the patches released to date, and it is his practice to promptly install any updates for which he sees an alert. Plaintiff expected the processor to function as Intel advertised and represented and to adequately secure stored data from exploits. Had Plaintiff known that in designing the CPU, Intel failed to take adequate measures to secure stored data, that it would not sufficiently monitor the security of its product, or that certain patches needed to address such security failures would result in the CPU's reduced performance, Plaintiff would not have bought the Acer laptop, or would have paid less for it.

40. **Plaintiff Sarah Stone** is a resident and citizen of the State of Oklahoma. In or about January 2010, Plaintiff bought a new Dell Experian desktop containing an Intel processor, and, in or about February 2014, Plaintiff bought a new Toshiba laptop containing an Intel Core i3 3120M CPU. Plaintiff's computers receive automatic updates that include the patches released to date. Plaintiff expected the processors to function as Intel advertised and represented and to adequately secure stored data from exploits. Had Plaintiff known that in designing its CPUs, Intel failed to take adequate measures to secure stored data, that it would not sufficiently monitor the security of its products, or that certain patches needed to address such security failures would result in the CPUs' reduced performance, Plaintiff would not have bought the computers, or would have paid less for each of them.

41. **Plaintiff Zachary Richard** is a resident and citizen of the Commonwealth of Pennsylvania. In or about November 2015, Plaintiff bought a new iBuypower desktop containing an Intel Core i7 6700 CPU. Plaintiff's desktop receives automatic updates that include the patches released to date. Plaintiff expected the processor to function as Intel advertised and represented and to adequately secure stored data from exploits. Had Plaintiff known that in designing the CPU, Intel failed to take adequate measures to secure stored data, that it would not sufficiently monitor the security of its product, or that certain patches needed to address such security failures would result in the CPU's reduced performance, Plaintiff would not have bought the iBuypower desktop, or would have paid less for it.

42. **Plaintiff Ashley Price** is a resident and citizen of the Commonwealth of Pennsylvania. In or about September 9, 2017, Plaintiff bought a new HP Envy laptop containing an Intel Core i5 7200U CPU. Plaintiff's laptop receives automatic updates that include the patches released to date. Plaintiff expected the processor to function as Intel advertised and represented

and to adequately secure stored data from exploits. Had Plaintiff known that in designing the CPU, Intel failed to take adequate measures to secure stored data, that it would not sufficiently monitor the security of its product, or that certain patches needed to address such security failures would result in the CPU's reduced performance, Plaintiff would not have bought the HP laptop, or would have paid less for it.

43. **Plaintiff John Nacci** is a resident and citizen of the State of Rhode Island. In or about 2010, Plaintiff bought a new HP Pavilion desktop containing an Intel Core 2 Quad Q6700 CPU. Plaintiff's desktop receives automatic updates that include the patches released to date. Plaintiff expected the processor to function as Intel advertised and represented and to adequately secure stored data from exploits. Had Plaintiff known that in designing the CPU, Intel failed to take adequate measures to secure stored data, that it would not sufficiently monitor the security of its product, or that certain patches needed to address such security failures would result in the CPU's reduced performance, Plaintiff would not have bought the HP desktop, or would have paid less for it.

44. **Plaintiff Kathleen Greer** is a resident and citizen of the State of South Carolina. In or about September 2017, Plaintiff bought a new Lenovo laptop containing an Intel Pentium 4405U CPU. Plaintiff's laptop receives automatic updates that include the patches released to date. Plaintiff expected the processor to function as Intel advertised and represented and to adequately secure stored data from exploits. Had Plaintiff known that in designing the CPU, Intel failed to take adequate measures to secure stored data, that it would not sufficiently monitor the security of its product, or that certain patches needed to address such security failures would result in the CPU's reduced performance, Plaintiff would not have bought the Lenovo laptop, or would have paid less for it.

45. **Plaintiff Jerry Peacock** is a resident and citizen of the State of South Dakota. In or about November 2016, Plaintiff bought a new Dell Inspiron laptop containing an Intel Core i5 6200U CPU. Plaintiff's Dell laptop receives automatic updates that include the patches released to date. Plaintiff expected the processor to function as Intel advertised and represented and to adequately secure stored data from exploits. Had Plaintiff known that in designing the CPU, Intel failed to take adequate measures to secure stored data, that it would not sufficiently monitor the security of its product, or that certain patches needed to address such security failures would result in the CPU's reduced performance, Plaintiff would not have bought the Dell laptop, or would have paid less for it.

46. **Plaintiff Matthew Ficarelli** is a resident and citizen of the State of Tennessee. In or about March 2017, Plaintiff bought a new Dell Inspiron All-in-One containing an Intel Core i3 6100U CPU, and, in or about April 2018, Plaintiff bought a new Dell Chromebook containing an Intel Celeron processor. Plaintiff's computers receive automatic updates that include the patches released to date. Plaintiff expected the processors to function as Intel advertised and represented and to adequately secure stored data from exploits. Had Plaintiff known that in designing its CPUs, Intel failed to take adequate measures to secure stored data, that it would not sufficiently monitor the security of its products, or that certain patches needed to address such security failures would result in the CPUs' reduced performance, Plaintiff would not have bought the computers, or would have paid less for each of them.

47. **Plaintiff DK Systems, LLC** is a resident and citizen of Wisconsin and provides IT services, including web hosting, to small businesses. From 1987 to present, Plaintiff bought servers and computers containing Intel CPUs. Plaintiff expected the processors to function as advertised and to adequately secure stored data from exploits. Had Plaintiff known that in

designing the CPUs, Intel failed to take adequate measures to secure stored data, that it would not sufficiently monitor the security of its products, or that certain patches needed to address such security failures would result in the CPU's reduced performance, Plaintiff would not have bought the aforementioned products containing the Intel CPUs, or would have paid less for them. Plaintiff has implemented patches released to date. Plaintiff has experienced performance degradation on various Intel-based systems, including reduced speed, and has expended significant resources on mitigation tasks as a result of Meltdown, Foreshadow and Spectre.

48. **Plaintiff Jessica Grosskopf** is a resident and citizen of the State of Wyoming. In or about August 2011, Plaintiff bought a new Dell laptop containing an Intel Core i5 2410M CPU. Plaintiff's laptop receives automatic updates that include the patches released to date. Plaintiff expected the processor to function as Intel advertised and represented and to adequately secure stored data from exploits. Had Plaintiff known that in designing the CPU, Intel failed to take adequate measures to secure stored data, that it would not sufficiently monitor the security of its product, or that certain patches needed to address such security failures would result in the CPU's reduced performance, Plaintiff would not have bought the Dell laptop, or would have paid less for it.

49. **Plaintiff Veronica Gardner** resident and citizen of the State of Arizona. In or about January 2011, Plaintiff bought a new HP Notebook containing an Intel Core i3 processor. Plaintiff's Notebook alerts her when an update is available, which she customarily installs promptly. Plaintiff also routinely manually double checks for available updates, ensuring her operating system is up to date, including the patches released to date. Plaintiff expected the processor to function as Intel advertised and represented and to adequately secure stored data from exploits. Had Plaintiff known that in designing the CPU, Intel failed to take adequate measures to

secure stored data, that it would not sufficiently monitor the security of its product, or that certain patches needed to address such security failures would result in the CPU's reduced performance, Plaintiff would not have bought the Notebook, or would have paid less for it.

50. **Plaintiff Hibbits Insurance, Inc.** ("Hibbits Insurance") provides insurance brokerage services and is organized under the laws of the state of South Carolina and primarily does business in South Carolina. Hibbits Insurance maintains a significant amount of private, sensitive and confidential information that it has a duty to protect from unauthorized access, including customer health information in connection with Hibbits Insurance's provision of health, dental, vision, disability income, and long-term care insurance services and consulting. During the class period, Hibbits Insurance purchased products containing defective Intel processors, including, but not limited to, i5, Celeron, and Pentium processors. Hibbits Insurance is obligated under federal and state laws and regulations, including the Health Insurance Portability and Accountability Act ("HIPAA") and the American Recovery and Reinvestment Act ("ARRA"), to maintain the privacy and security of its customers' health information. HIPAA-covered entities like Hibbits Insurance have received notices from the federal government warning of the Meltdown and Spectre security vulnerabilities. Moreover, Hibbits Insurance also provides property and casualty insurance services and consulting, which also requires safeguarding confidential information of customers. Federal statutes, like the Gramm-Leach-Bliley Act, require insurance-related entities and financial institutions to evaluate potential security threats, like those posed by the Spectre and Meltdown vulnerabilities, and protect against the unauthorized use or disclosure of nonpublic personal financial data. Hibbits Insurance expected its Intel processors to function as represented or advertised by Intel and to adequately secure stored data from exploits. Had Hibbits Insurance known that in designing the CPUs, Intel failed to take adequate

measures to prevent unauthorized access to stored data, that it would not sufficiently test and monitor the security of its products, or that certain patches needed to address such security failures would result in the CPU's reduced performance, Hibbits Insurance would not have purchased devices containing the defective Intel CPUs, or would have paid less for them. As a result of the Defects, Hibbits Insurance has incurred and will continue to incur time and costs because it has been and will continue to be required to, among other things: increase monitoring of the Affected Devices for security threats, attacks and breaches; implement mitigation and remedial measures, such as patching to address the security vulnerabilities; monitor and test new patches and firmware updates; supplement its and computing security program(s) with additional security monitoring; and replace or upgrade products with affected processors on an accelerated schedule.

51. **Plaintiff Daren Rexroad** is a resident and citizen of the State of Vermont. From 2011 through 2015, Plaintiff purchased a Macbook Pro with an Intel Core I7, two 13" Macbook Airs with Intel Cores I5, and an 11" Macbook Air with an Intel Core I5. Plaintiff's computers receive automatic updates that include the patches released to date. Plaintiff expected the processors to function as Intel represented and advertised and to adequately secure stored data from exploits. Had Plaintiff known that in designing the CPU, Intel failed to take adequate measures to secure stored data, that it would not sufficiently monitor the security of its product, or that certain patches needed to address such security failures would result in the CPU's reduced performance, Plaintiff would not have bought the computers, or would have paid less for them.

52. **Plaintiff Barry Wayne Browning** is a resident and citizen of the State of West Virginia. In or about 2010, Plaintiff bought a Dell Model PP29L Inspiron laptop computer. In or about 2012, Plaintiff bought a Dell Model P25F Inspiron laptop computer. Plaintiff receives automatic updates that include the patches released to date. Plaintiff expected the processor in both

computers to function as Intel represented and advertised and to adequately secure stored data from exploits. Had Plaintiff known that in designing the CPU, Intel failed to take adequate measures to secure stored data, that it would not sufficiently monitor the security of its product, or that certain patches needed to address such security failures would result in the CPU's reduced performance, Plaintiff would not have bought either computer or would have paid less for it.

CHOICE OF LAW

53. The application of California law to this litigation is appropriate given Intel's connection to the State of California since the 1970s. As Intel itself states:

> We purchased our first piece of property—a 26-acre pear orchard on the corner of Coffin Road and Central Expressway in Santa Clara, California in 1970. Today, we have 15,000 employees across the state at three major sites in Santa Clara, San Jose, and Folsom, and at research and development sites in Irvine and San Diego. Santa Clara is home to Intel's corporate headquarters and the flagship Intel Museum, which showcases five decades of Intel® innovations.[1]

54. Intel boasts that it has "invested in California for five decades, since our founding in Mountain View in 1968."[2]

55. But Intel's connection to California does not end in Santa Clara. It has divisions throughout the State, including in Folsom.

56. Intel states that its "Folsom site is a center of excellence for graphics, chipsets and solid state drives, delivering innovative technology and support for a wide range of devices and client platforms. With close to 6,000 employees, Intel is Folsom's largest private sector employer, and one of the Sacramento region's top 5 private employers."[3]

[1] Intel in California, https://www.intel.com/content/www/us/en/corporate-responsibility/intel-in-california.html (last accessed Aug, 21, 2018).

[2] *Id.*

[3] *Id.*

57. Intel's Santa Clara site, however, is where the fraudulent conduct as described herein originated. As Intel states, "The Santa Clara site is involved in engineering, design, research and development, and software engineering, and houses several corporate organizations, including sales and marketing, legal, supply chain, and human resources. With more than 6,500 employees, Intel is one of the largest employers in Santa Clara."[4]

58. Intel's own website even shows that nearly all of its available marketing jobs in the United States—the very arm of the company that would have been responsible for the consumer-facing advertisements, representations, and even omissions—are located in the State of California.[5]

59. The State of California has a substantial interest in ensuring that corporations do not misrepresent their products, omit security risks concerning those products, and otherwise engage in business decisions that would harm consumers.

60. The application of California law to Intel—a California company that took substantial actions in the State of California impacting Plaintiffs and the Class members in the State of California—would neither be unfair, unlawful, or unconstitutional.

SUBSTANTIVE ALLEGATIONS

A. General Background

1. Intel's 8086 and x86 Instruction Set

61. Intel, a portmanteau of the words "integrated" and "electronics," was founded by Robert Noyce and Gordon Moore in 1968 for the purpose of designing and manufacturing memory

[4] *Id.*

[5] Intel Job Openings for "Marketing" Positions, https://jobs.intel.com/ListJobs/All/Search/jobtitle/marketing/ (last accessed Aug. 21, 2018).

devices for computers utilizing silicon, a semiconducting material and one of the common elements found on Earth. In 1971, the Company went public and has been traded on the NASDAQ continuously ever since. That same year, Intel launched the first commercially available microprocessor, the Intel 4004.

62. A microprocessor is an integrated electronic circuit that contains all the functions of a central processing unit ("CPU") of a computer. The CPU is the "brains" of the computing device, performing all necessary computations for each application (e.g., Microsoft Word) and each peripheral (e.g., a printer). Each program communicates with the processor through instructions, with each instruction representing a calculation or operation that the CPU must execute on behalf of the requesting application. For each calculation, the CPU "fetches" the instruction from the computer's memory, "decodes" it, "executes" it, and, finally, "writes-back" the result. The time it takes a CPU to process instructions is measured in "clock cycles." Each step in the process—fetch, decode, execute, and write-back—takes at least one clock cycle. The number of clock cycles a CPU completes per second is known as the "clock rate." "Clock speed" or "frequency" is a way to measure a CPU's processing speed and is usually expressed in megahertz ("MHz") or gigahertz ("GHz").

63. In 1978, Intel debuted the 8086 microprocessor. The 8086 was a 5 Mhz, 16-bit processor, capable of handling up to 1 megabyte ("MB") of data.[6] For the 8086, Intel designed an "instruction set," known as x86, and a "microarchitecture," known as 8086. The instruction set serves as an interface between a computer's software and hardware. The microarchitecture governs the various parts of the processor and how they work together to implement the instruction set.

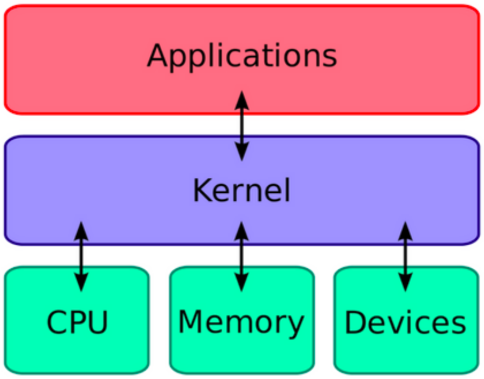
[6] A "bit" is the smallest unit of storage. A "byte" is equal to 8 bits.

64. In July 1981, IBM launched its first personal computer ("PC"), powered by Intel's 8088 microprocessor, a more economical version of the 8086 microprocessor, also based on the x86 instruction set. Because IBM allowed manufacturers or OEMs to clone its PC design, IBM PCs and clones thereof soon dominated the market. Each of these computers was powered by a processor that implemented Intel's x86 instruction set. Today, the majority of all PCs, laptops, workstations, and servers are powered by processors based on Intel's x86 instruction set.

2. Intel's 80286 and the Introduction of Protected Mode

65. In 1982, Intel released its second-generation processor based on the x86 instruction set, the 80286. Before the 80286, processors had one operation mode known as "real mode." When the computer operated in real mode, applications had unlimited and direct access to all of a computer's memory, including information stored in the "kernel."

66. The kernel is the central part of the computer's operating system ("OS"). Notable OS include Microsoft Windows, Linux, and Apple's MacOSx. As demonstrated in the graphic below, the kernel acts as the intermediary between the CPU, memory, and any applications or peripherals:

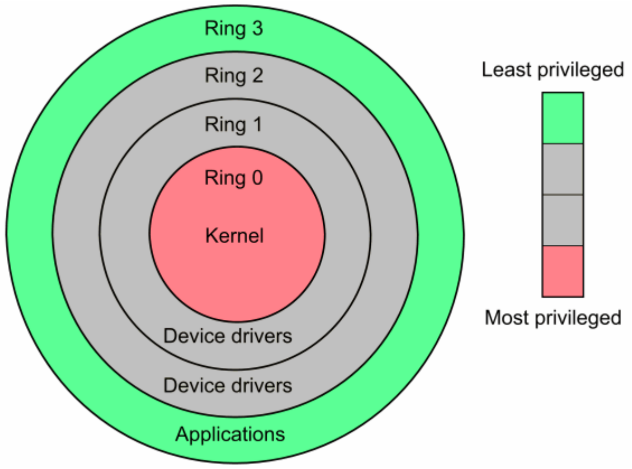


67. When a computer is operating in real mode, it is possible for a malfunctioning or malignant application to access the kernel and overwrite the OS, leading to catastrophic failure of

the computer. Today, such a failure could lead to "kernel panic" or, on a computer running Windows, the feared "Blue Screen of Death," which is displayed if the OS experiences a fatal system error.

68. In order to minimize OS failures, Intel's 80286 introduced the concepts of "protected mode" and "virtual memory." Protected mode allows the OS to remain in control of the computer through the kernel. "Virtual memory" allows the computer to segment its physical memory into separate spaces, including "kernel space," where the computer runs and stores the critical kernel code, and "user space," where the computer runs and stores all of the other code needed to run the applications and peripherals.

69. The relevant importance of the code is determined by utilizing the concept of "protection rings." As demonstrated in the graphic below, "Ring 0" includes the most privileged information, which resides in the kernel, while "Ring 3," includes the least privileged information, which is accessible to virtually all applications:



70. Access to these spaces is controlled by a program's "privilege level." To protect the computer's most privileged information (Ring 0), engineers rely on the "principle of least privilege," meaning that every program only has access to the least amount of privileged

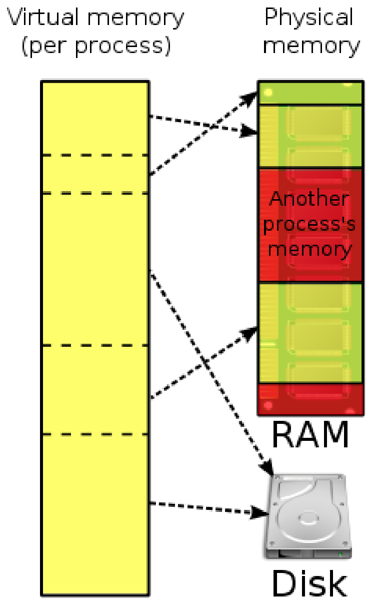
information it needs to perform its intended function. Typically, before a CPU fetches instructions or data requested by an application, the computer must first determine whether that program has the requisite privilege level to access that information. If the application does not have permission to access the requested instructions or data, an exception occurs within the CPU and the request fails.

71. The privilege levels defined in the x86 instruction set are meant to ensure that programs other than the kernel do not have direct access to a computer's most privileged information and that, if access is required, it is controlled by and is initiated through the kernel. This ensures that no application can access a computer's Ring 0 information or make changes to the OS without involving the kernel.

72. With the launch of the 80386 processor in October 1985, the functionality of protected mode and virtual memory was improved, and to this day all modern processors utilize these functionalities to protect the computer's most privileged information.[7]

73. With virtual memory, each user process has its own virtual address space, which creates the illusion that each user has a memory space much larger than the physical, hardware-backed memory actually available on the machine. In fact, user processes are sharing the limited physical memory, and portions of each program's instructions or data may actually be located in secondary storage (*e.g.*, on disk).

[7] The Intel Trinity by Michael S. Malone.



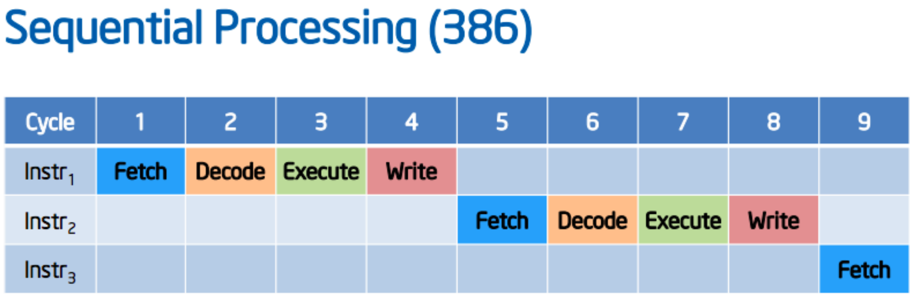
74. The virtual address space allows each program to believe it is the only one (aside from the kernel (OS)) that is running on the machine. This helps prevent applications from crashing and it also serves a security function by isolating processes from each other. User applications should not be able to access each other's memory, or read or write to kernel memory, without permission. This allows multiple applications to run simultaneously on personal devices and multiple users to execute processes on the same machine in the cloud.

75. When a processor seeks to access data or instructions from memory, a virtual address has to be translated into a physical address to determine where the information is located. Page tables are used to map the virtual to physical addresses, translating the virtual addresses seen by an application into physical addresses used by the hardware.

3. Intel's 80486 and the Introduction of Pipelines and On-Die Caches

76. Intel introduced the next generation of the x86-based processor, the 80486, in 1989. The 80846 boasted twice the performance of the 80386, due in part to two key improvements to the microarchitecture: pipelines and on-die caches.[8]

77. **Instruction Pipelining.** Earlier iterations of Intel's x86-based processors utilized "sequential" processing, working through each step of the first instruction (e.g., fetch, decode, execute, and write-back) before starting the next instruction. The following diagram reflects the 80386's sequential processing. In this example, it takes eight clock cycles to complete two instructions:

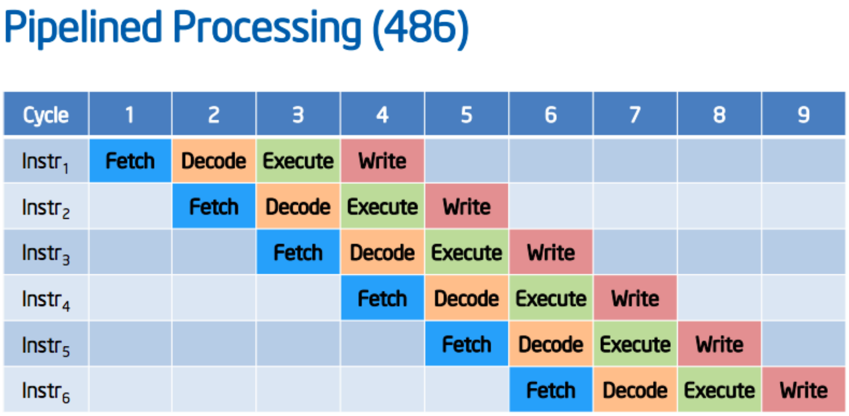


Sequential Processing (386)

Cycle	1	2	3	4	5	6	7	8	9
Instr$_1$	Fetch	Decode	Execute	Write					
Instr$_2$					Fetch	Decode	Execute	Write	
Instr$_3$									Fetch

78. The 80486 was a "pipelined" processor, meaning that the CPU began processing the next instruction before it had completed processing the prior instruction. As reflected in the diagram below, on Clock Cycle 2, the 80486 was able to both decode the instruction fetched during Clock Cycle 1, and fetch the next instruction. With pipelining, the 80486 could complete six instructions in nine clock cycles, nearly tripling the work completed in the same amount of time:

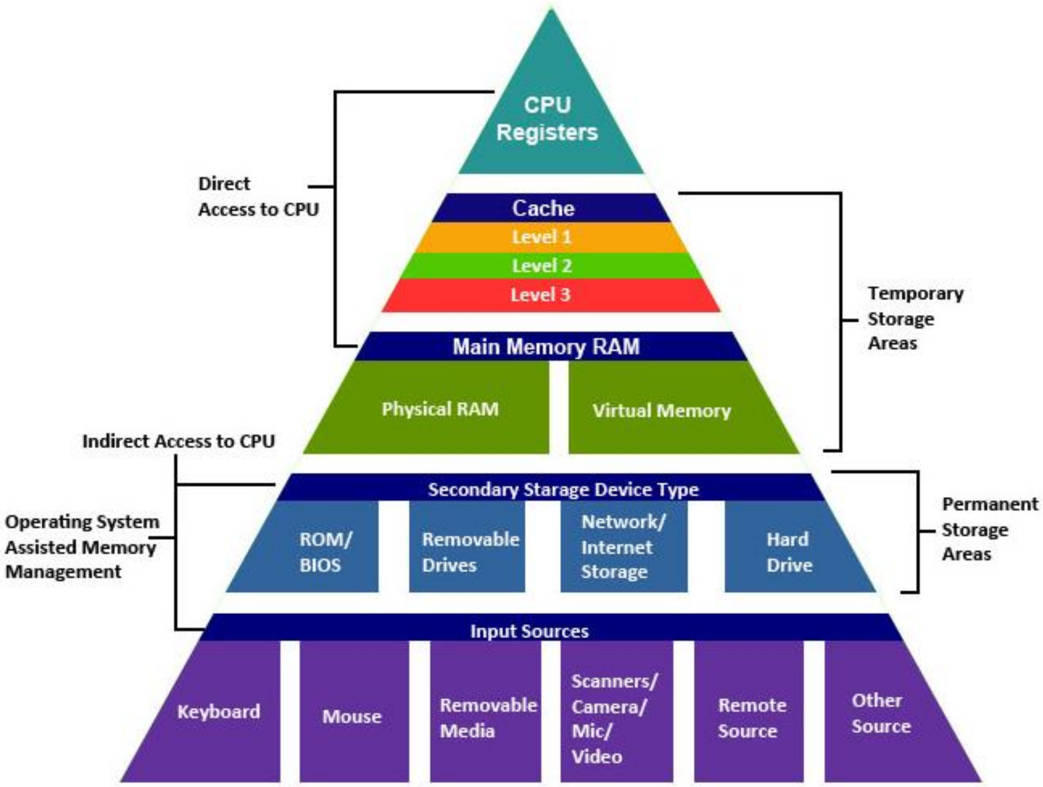
[8] The Intel Trinity by Michael S. Malone.



Pipelined Processing (486)

Cycle	1	2	3	4	5	6	7	8	9
Instr$_1$	Fetch	Decode	Execute	Write					
Instr$_2$		Fetch	Decode	Execute	Write				
Instr$_3$			Fetch	Decode	Execute	Write			
Instr$_4$				Fetch	Decode	Execute	Write		
Instr$_5$					Fetch	Decode	Execute	Write	
Instr$_6$						Fetch	Decode	Execute	Write

79. **Memory Hierarchy and On-Die Caches.** A computer's memory system, which holds instructions and data for the CPU, is a hierarchy of storage devices with different capacities and access times. When the CPU needs instructions or data to complete a task, it must fetch it from memory. The following pyramid helps depict the basic memory hierarchy:



80. Data in the CPU registers can be operated on immediately during execution by the CPU.

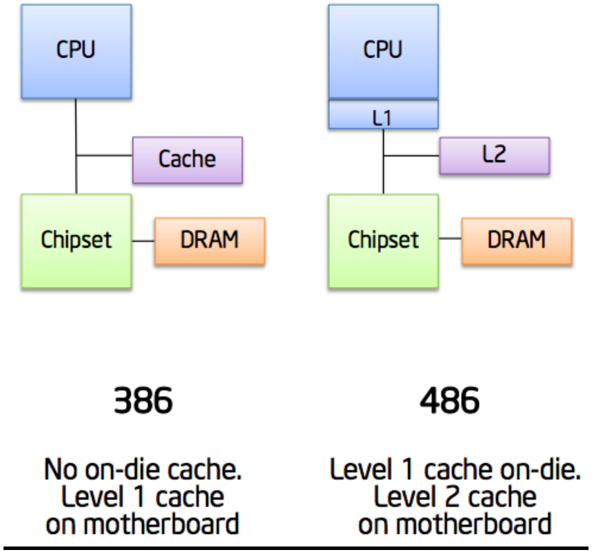
81. A computer's physical memory space—known as "main memory"—is separated from the CPU on the computer's main circuit board or motherboard. Fetching instructions or data from main memory is highly inefficient because main memory runs at a slower speed than the CPU (the "performance gap") and because of the time it takes for information and data to travel between main memory and the CPU on the motherboard ("latency").

82. In order to mitigate the performance gap and the issue of latency, modern microarchitecture designs rely on caches. A "cache" is a location between main memory and the CPU that can be used to temporarily store information and data for the use of the CPU. Caches typically operate at the same or similar speed as the CPU, mitigating the performance gap. Caches also are located in closer proximity to the CPU, addressing the latency problem. As a result, when a processor needs to fetch instructions or data, it can first check to see if the necessary information has been stored in the cache. If the information is in the cache (a "cache hit"), the CPU avoids the delay and associated performance penalty associated with fetching the information from main memory. If the information is not in the cache (a "cache miss"), the CPU fetches it from main memory.[9]

83. Because caches help minimize delays associated with fetching information from main memory, a processor with at least one cache typically is faster than a processor without any caches. While prior generations of Intel's x86-based processors included a first level or "L1" cache between main memory (referred to as "DRAM" in the diagram below) and the CPU on the

[9] Worse yet, if not present in main memory, the data or instructions must be fetched from storage, e.g., disk, which is even slower.

motherboard, the 80486 brought the L1 cache onto the same "die" (or piece of silicon) as the CPU and added a separate second level or "L2" cache to the motherboard:



84. By placing the L1 cache directly on the CPU die, the 80486 further decreased the time needed to fetch instructions and data, improving latency. By adding a second cache, the increased overall cache capacity made it more likely the CPU would find the information it needed in one of the caches, without having to resort to fetching it from main memory.

85. However, despite the 80486's clear performance advantage, Intel struggled to convince OEMs to launch PCs powered by the 80486 or to convince end-users that they needed a more powerful processor than the 80286 or 80386. At the time, PCs were utilized at most for word processing, which simply did not require the fire-power of Intel's next generation of x86-based processors, and the market had not yet accepted the idea that technology could be rendered obsolete within two to three years of its introduction.

86. To make matters worse, at the end of 1990, Intel's largest competitor, Advanced Micro Devices, Inc. ("AMD") launched a clone of Intel's 80386 microprocessor, the AM386, which was faster and cheaper than Intel's 80386. Notably, this was not the first time that AMD

had launched a faster clone of an Intel processor. With the 80286, IBM required Intel to use AMD as a second supply source, effectively forcing Intel to give to its competitor a license to the 80286 code. This was not a good development for Intel: AMD's 80286 clone, the AM286, could run as fast as 25 MHz, while Intel's 80286 processors clocked between 6 MHz and 12 MHz.[10] As a result, when Intel subsequently launched the 80386, the Company refused to grant AMD a license.

87. In response to the success (and speed) of the AM386, Intel sued AMD and launched a $250 million multi-media "Intel Inside"-based campaign to push the end-users to demand from the OEMs PCs powered by the 80486. Intel had started its "Intel Inside" campaign in 1989 by asking PC makers, including IBM, to place "Intel Inside" stickers on the computers themselves to generate brand-loyalty among the end-users.[11] The goal of the campaign was to educate consumers as to the reliability and superior performance of Intel-branded processors and to ensure that they could differentiate between an Intel processor and a clone sold by one of its competitors. As Intel's former CEO, Andrew Grove described it, "Intel Inside" drove home the point "that the identity and class of the computer were determined more than anything else by the microprocessor within."[12]

88. The campaign worked. Not only did customer-pressure lead to OEMs announcing new PCs powered by Intel's 80486, but many of the manufacturers agreed to use the "Intel Inside" branding in their own marketing efforts. By 1997, 1,500 OEMs were incorporating the "Intel

[10] The Intel Trinity by Michael S. Malone.

[11] http://articles.latimes.com/1991-11-02/business/fi-797_1_advertising-campaign (last visited Aug. 24, 2018)

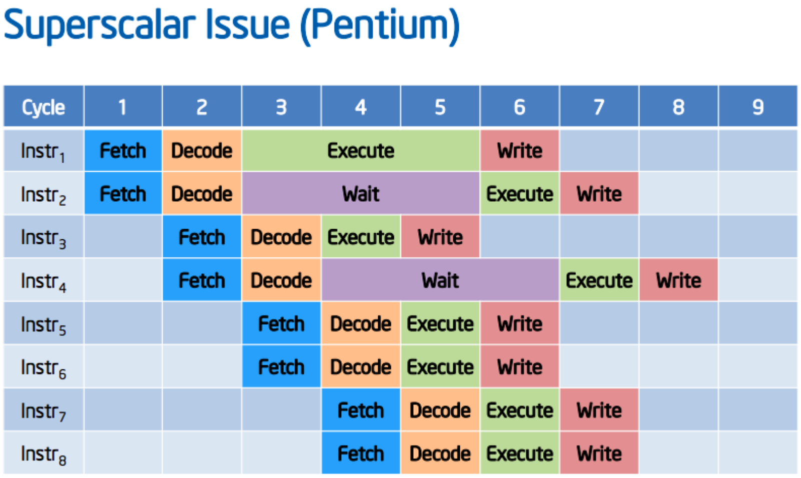
[12] Only the Paranoid Survive: How to Exploit the Crisis Points That Challenge Every Company by Andrew S. Grove.

Inside" theme into their marketing efforts.[13] By 2000, Intel was the second-best-known industrial brand (after Coca-Cola) in the world.[14]

4. Intel's P5 Microarchitecture

89. In 1993, Intel introduced its fifth-generation microarchitecture based on the x86 instruction set, known as P5. Intel launched the "Pentium"-branded processors based on P5.

90. The P5-based processors were significantly faster due to their superscalar design. Whereas pipelining allowed a CPU to process different aspects of multiple instructions at the same time, a superscalar design allowed the CPU to fetch two instructions at the same time, decode two instructions at the same time, and so forth. A pipelined superscalar design, such as the P5-based Pentium processor, allowed the processor to decode Instructions 1 and 2, while fetching Instructions 3 and 4:



Superscalar Issue (Pentium)

Cycle	1	2	3	4	5	6	7	8	9
Instr$_1$	Fetch	Decode	Execute			Write			
Instr$_2$	Fetch	Decode	Wait			Execute	Write		
Instr$_3$		Fetch	Decode	Execute	Write				
Instr$_4$		Fetch	Decode	Wait			Execute	Write	
Instr$_5$			Fetch	Decode	Execute	Write			
Instr$_6$			Fetch	Decode	Execute	Write			
Instr$_7$				Fetch	Decode	Execute	Write		
Instr$_8$				Fetch	Decode	Execute	Write		

91. As compared to a sequential processor (e.g., the 80386 at two instructions in eight clock cycles), and a pipelined processor (e.g., the 80486 at six instructions in nine clock cycles), a superscalar pipelined processor could complete eight instructions in eight clock cycles.

[13] http://adage.com/article/adage-encyclopedia/intel-corp/98721/ (last visited Aug. 24, 2018)

[14] The Intel Trinity by Michael S. Malone.

92. Intel used its "Intel Inside" campaign to make "Pentium" a household name. However, the success of the campaign became a curse once Intel discovered, in the summer of 1994, that Pentium had a design flaw. Intel initially decided not to publicly disclose the Defect because it believed very few customers would be impacted. However, the flaw was later uncovered by a North Carolina professor in October 1994, ultimately leading to intense media scrutiny. The *Wall Street Journal*'s principal technology columnist, Walter Mossberg, described the scandal as worse than Watergate. IBM, in turn, suspended shipment of all Pentium-powered PCs on December 12, 1994, because its independent research confirmed the flaw was more serious than Intel had claimed.[15]

93. At first, Intel resisted public pressure to conduct a full recall, continuing to sell the flawed Pentium and agreeing only to issue replacements if consumers could demonstrate that they were likely to encounter the flaw. However, on December 19, 1994, one week after IBM suspended shipments of Pentium-powered PCs, Intel finally agreed to a full recall. On January 17, 1995, Intel announced that it would spend $475 million to replace the flawed processors and that, going forward, Intel would immediately disclose any and all defects in its future microprocessors.[16]

5. Intel's P6 and the Introduction of Dynamic Execution

94. Intel introduced its P6 architecture in November 1995. Makers of large computers, servers, and workstations quickly embraced the P6-based Pentium Pro processors.[17] In 1997, Intel

[15] The Intel Trinity by Michael S. Malone.

[16] The Intel Trinity by Michael S. Malone.

[17] The Intel Trinity by Michael S. Malone.

also successfully launched the Pentium II processor, a more consumer-oriented processor based on the P6 architecture.

95. In a number of ways, the P6 microarchitecture represented a break from Intel's prior x86-based designs. As explained by Intel on its launch, the P6 "microarchitecture was tuned to what was proven performance," "[o]ptimizing CPI [clock per instruction] and [f]requency" to achieve a "50% frequency gain," and, ultimately, a "37% performance gain." In designing the P6 microarchitecture, Intel determined that "Dynamic Execution," which included the concepts of "out-of-order execution," "speculative execution," and "branch prediction" was "required for higher performance."[18]

96. **Out-of-Order Execution.** Every application or program has a set of instructions that it wants the CPU to execute in order ("program order"). These instructions require the CPU to, for example, engage in arithmetic or logical functions.

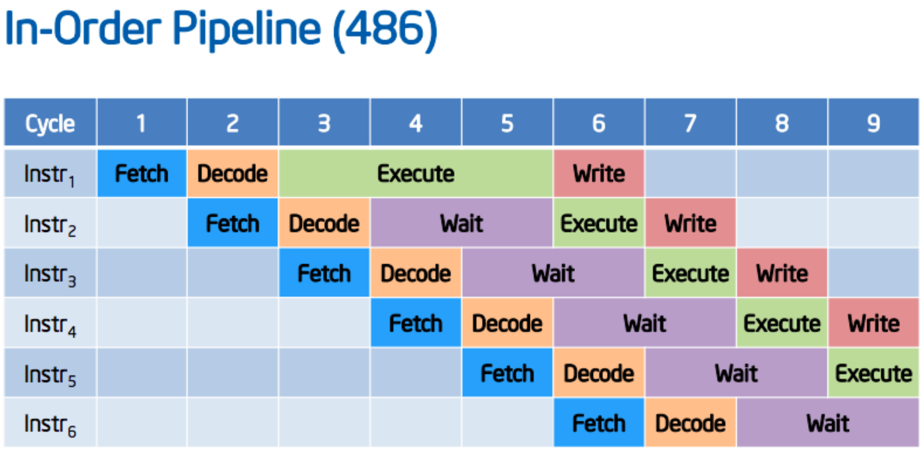
97. Instructions can be "data dependent," meaning that the instruction needs the data produced by a preceding instruction in order to execute. For example, suppose the CPU needs to add four numbers together: 1, 32, 75, and 89. Instruction 1 can add the first two numbers (1+32=33) and Instruction 2 can add the second two numbers (75+89=164). Instruction 3, however, is a data dependent instruction because the CPU needs the results of Instruction 1 (33) and Instruction 2 (164) to execute it.

98. Instructions also can be "conditional" expressed as, "if X, then Y." For instance, Microsoft Word has an autocorrect feature that determines whether a word is spelled correctly after it is typed. If the word is spelled incorrectly, the program fixes it. In that scenario, the conditional instruction is, "If a word is misspelled (X), then fix it (Y)." With Word's autocorrect

[18] "Optimizing the P6 Pipeline," Intel presentation at 1995 Hot Chips conference.

feature, there are two possibilities or "branches"—there is a misspelling which needs to be fixed, or there is no misspelling and the CPU can move on to another instruction. A conditional instruction has to be resolved before the CPU can determine the next step or branch to take. For this reason, such conditional instructions are sometimes called "branch instructions."

99. Data dependent and conditional instructions (among others) can take a number of clock cycles to execute, leading the CPU to "stall" while it waits for the necessary data or branch it should follow to execute the next instruction. The diagram below shows "in-order" execution in an 80486 pipelined processor where the CPU is stalled with respect to Instructions 2-6. When Instruction 1 takes six clock cycles, only three instructions are complete at the end of eight clock cycles, as compared to five instructions after eight clock cycles where there is no CPU stall.

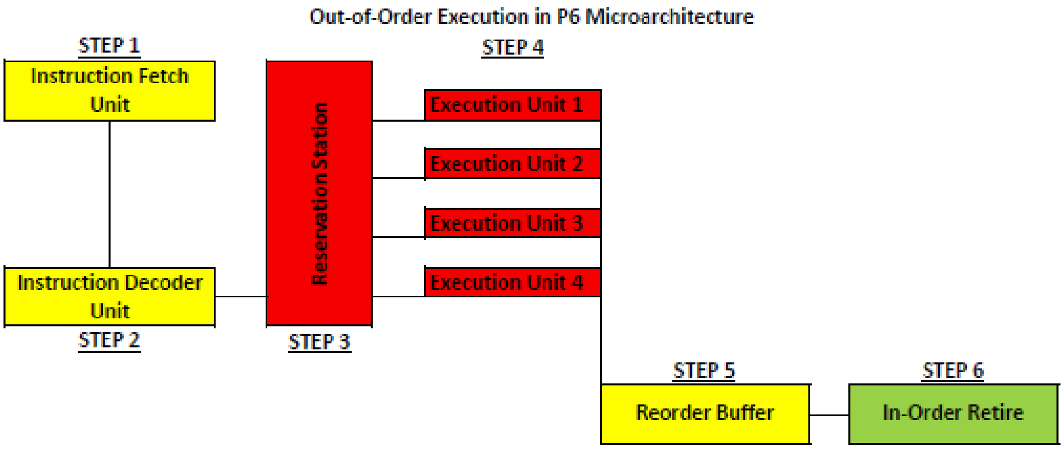


In-Order Pipeline (486)

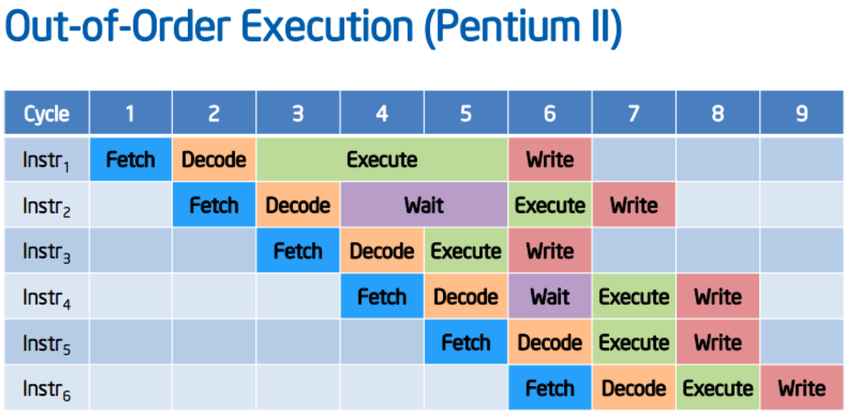
Cycle	1	2	3	4	5	6	7	8	9
Instr$_1$	Fetch	Decode	Execute			Write			
Instr$_2$		Fetch	Decode	Wait		Execute	Write		
Instr$_3$			Fetch	Decode	Wait		Execute	Write	
Instr$_4$				Fetch	Decode	Wait		Execute	Write
Instr$_5$					Fetch	Decode	Wait		Execute
Instr$_6$						Fetch	Decode	Wait	

100. Out-of-order execution ("OoOE") addresses this problem. Instead of executing each instruction in "program order," the CPU executes instructions based on "dataflow order," or, in other words, the CPU executes instructions based on an order determined by what data is available to it at any given time. Dataflow order is akin to what students are taught to do with standardized tests—complete questions for which the answer is known first, before going back to those questions for which the answer is not clear.

101. The following diagram shows OoOE in the P6 microarchitecture. In Steps 1 and 2, the instructions are fetched, decoded, and moved to the Reservation Station. In Step 3, the Reservation Station sends instructions in dataflow order to the Execution Units. During Step 4, the Execution Units execute the instructions and send the results to the Reorder Buffer. Information necessary to execute these instructions is held in the processor's cache. The Reorder Buffer puts the instructions back into "program order" (Step 5) and sends them to be retired in order (Step 6).



102. With OoOE, P6-based processors can overcome the CPU stall generated by Instruction 1 in the image below and execute five instructions in eight clock cycles, eliminating the performance penalty and speeding up the processor.



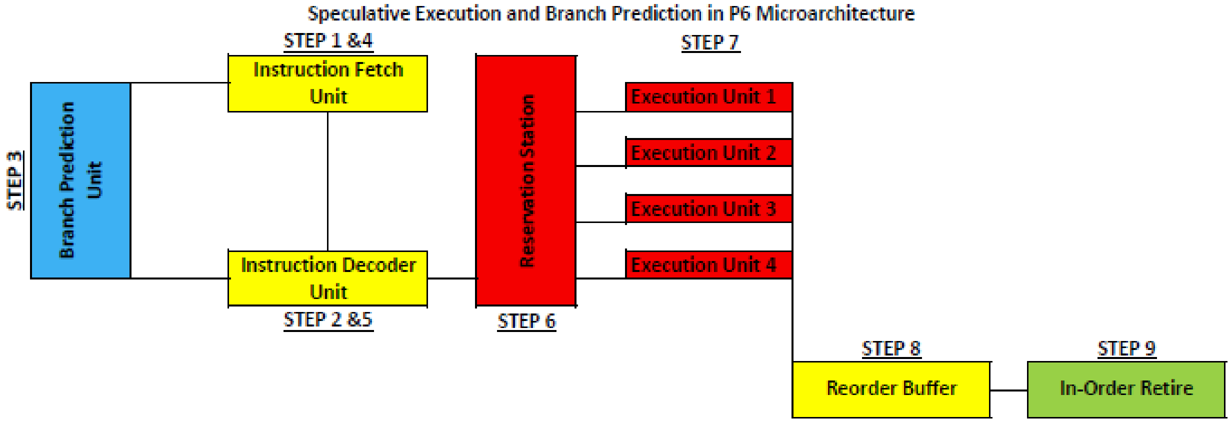
Out-of-Order Execution (Pentium II)

Cycle	1	2	3	4	5	6	7	8	9
Instr_1	Fetch	Decode	Execute			Write			
Instr_2		Fetch	Decode	Wait		Execute	Write		
Instr_3			Fetch	Decode	Execute	Write			
Instr_4				Fetch	Decode	Wait	Execute	Write	
Instr_5					Fetch	Decode	Execute	Write	
Instr_6						Fetch	Decode	Execute	Write

103. Ultimately, Intel concluded that OoOE was helpful, because it "allowed higher clock frequency without CPI [average clock cycles per instruction] degradation" and "provid[ed] more performance per square mil of datapath."[19]

104. **Branch Prediction and Speculative Execution.** While OoOE improves the performance of a processor by mitigating CPU stalls generated by data dependent instructions, only branch prediction and speculative execution ameliorate the performance impact of conditional instructions on the CPU. When the CPU fetches and decodes a conditional instruction, the processor predicts the "branch" based on prior results and then speculatively executes instructions down that branch until the conditional instruction is executed and the branch is resolved.

105. The following diagram demonstrates branch prediction and speculative execution in the P6 microarchitecture. If a conditional instruction is fetched and decoded (Steps 1 and 2), then the Branch Prediction Unit (Step 3) is queried, with the resulting guess going to the Instruction Fetch Unit in Step 4. From there, the processor decodes and speculatively executes the instructions down the predicted branch (Steps 5-7). Meanwhile, the information for these speculatively executed instructions is stored in the processor's caches.



[19] "Optimizing the P6 Pipeline," Intel presentation at 1995 Hot Chips conference.

106. When the CPU eventually executes the conditional instruction, the processor checks whether its prediction was correct. If the Branch Prediction Unit guessed correctly, the processor has performed useful work and the results are written to memory (Step 9, above). If the CPU guessed incorrectly—a "mispredicted branch"—the processor "flushes" its pipeline of the impact of the speculatively executed instructions and proceeds to execute the instructions from the correct path. Critically, and as further explained in Section B, according to Intel's microarchitecture design, the CPU does not flush its cache after a mispredicted branch and so the information associated with the speculative execution down the incorrect branch remains in the processor.

6. The Netburst Microarchitecture Disaster

107. The speed at which a CPU performs is a material attribute for consumers purchasing a desktop, laptop, workstation, or server powered by an Intel processor. Without sufficient processing speed, a CPU will be unable to effectively and efficiently run the device's OS and applications, or utilize connected hardware and peripherals. As a result of Intel's various direct-to-consumer marketing campaigns, including "Intel Inside," consumers look to and rely upon the processor's advertised clock speed to measure a CPU's performance. Intel's focus on clock speed in its marketing led to the "Megahertz Wars," followed by the "Gigahertz Wars," during which Intel and its main competitor, AMD, battled to see which company could achieve the fastest clock speed.

108. After successfully cloning the 80286, 80386, and 80486, AMD launched its own x86-based microarchitecture design, K5, in 1995. Like Intel's P6, AMD's microarchitecture designs relied upon OoOE, speculative execution, and branch prediction to achieve performance increases over earlier generations of processors. In July 1999 AMD took the "speed crown" from

Intel with the launch of its K7-based Athlon-branded processors.[20] Thereafter, the title of the fastest processor changed hands several times.

109. Then in March 2000, AMD successfully launched the first processor that could reach 1 GHz. Desperate to also reach the coveted goal of 1 GHz, Intel resorted to introducing the 1 GHz P6-based Pentium III processor just two days later, well before the Company was ready to ship these processors, as well as the previously-announced 850, 866, and 933 MHz P6-based Pentium III processors to consumers. Intel quickly followed this much-derided "paper launch" by announcing a 1.13 GHz Pentium III in July 2000.[21]

110. However, problems with the 1.13 GHz Pentium III on the test bench led tech reviewers to publicly conclude that Intel had serious production issues with its 1.13 GHz CPU. After a third outlet, *AnandTech*, came forward, confirming these reports, Intel recalled the 1.13 GHz Pentium III in August 2000, approximately one week after the first shipments of these processors reached customers.

111. Hoping to outrun the negative press it had generated over the last year, Intel announced its newest microarchitecture, Netburst and Netburst-based Pentium 4 processors in November 2000. According to Intel, Netburst-based CPUs "feature[d] significantly higher clock rates and world-class performance."

112. Although the original Pentium 4 processors clocked at just over 1 GHz, Intel designed the Netburst microarchitecture with room to allow successive processors to reach clock speeds of up to 10 GHz. To reach these speeds, Netburst included an improved cache subsystem, featuring larger, faster caches, a deeply pipelined design (doubling the number of pipeline stages),

[20] https://www.anandtech.com/show/613/2 (last visited Aug. 24, 2018).

[21] https://www.anandtech.com/show/613/2 (last visited Aug. 24, 2018).

and "hyper-threading" technology, to ensure that the CPU was effectively and efficiently taking advantage of all available resources to achieve increased frequency and performance benchmarks.

113. Intel designed the first Netburst-based processors, Pentium 4s code-named "Willamette," to reach clock speeds of 1.5 GHz. However, the Willamette processors could not outscore the P6-based Pentium IIIs or AMD's Athlon processors in commercially available benchmark testing. In a lawsuit filed in 2002 in California state court, styled *Skold v. Intel Cor.*, No. 1-05-CV-039231 (hereafter "*Skold*"), consumers who ultimately purchased computers powered by the Willamette processors alleged that the "Pentium 4's scores were so bad that Intel [internally] deemed it 'not competitive' with AMD's Athlon processor or . . . [the] Pentium III processor, noting that most benchmark tests showed a 'negative or zero performance gain.'"

114. According to the plaintiffs in *Skold*, the Willamette processors performed poorly due to "design flaws" in the Netburst architecture, which "Intel admitted . . . were so serious and so pervasive that they would significantly impair any computer's performance by dramatically slowing its ability to process the computer's instructions." These flaws were the result of "a 'complete failure' of the design process," requiring "a dramatic change in [Intel's] engineering" process and a redesign that would prevent Intel from releasing a new processor for another two years.

115. With AMD already taking market share, Intel could not wait until 2002 to launch a competitive processor. With "Intel Inside," the Company had conditioned consumers to look to Intel for superior performance and reliability. By focusing on processing speed and commercial benchmarking, Intel likewise had conditioned the market to focus on clock speed to measure a processor's performance and determine which computer to purchase. And, critically, Intel priced

its processors based on the market's perception of its performance. In fact, Intel was able to garner a premium for its processors throughout the 1990s.

116. However, if Intel released the Willamette processors, the public would soon learn what the Company already had discovered internally: the Pentium 4 was an overpriced dud. As alleged in *Skold*, "Intel solved its problem by making it *appear* as if the [Willamette processor] outscored the Pentium III and AMD Athlon processors" by inflating its performance scores after it publicly launched the processor. This strategy included surreptitiously developing a new, purportedly independent benchmark and altering another purportedly independent benchmark to fool consumers into thinking that Intel's Willamette processor out-performed the Pentium III and AMD processors. Intel also disabled features on the Pentium III, hobbling its performance so that the Willamette processors would appear faster by comparison. OEMs like HP were incentivized to help Intel with its deception to sell more computers.

117. Ultimately, Intel settled the lawsuit in 2014, agreeing to pay a 49-state class of consumers who purchased a computer powered by a Willamette processor $15 per device.

7. Intel's Core Microarchitecture

118. After the Willamette debacle, Intel tried several times (without success) to release a number of processors based on the Netburst microarchitecture in response to AMD's successful products, including dual-core Athlon and Opteron processors. In a last-ditch attempt to make Netburst work, Intel designed, tested, and launched in just nine months, "Smithfield," a dual-core, high-end Netburst-based processor. By August 2005, as reported by PCWorld, Intel publicly admitted that its "first dual-core [processor] was a hastily concocted design that was rushed out the door in hopes of beating rival . . . [AMD] to the punch."[22]

[22] https://www.pcworld.com/article/122236/article.html (last visited Aug. 24, 2018).

119. The failed Smithfield launch made it clear that Intel had hit a wall. Where Intel was once able to announce materially increased clock speeds with each new processor, now it was lucky if it could eke out a single-digit percentage increase. Intel's designs could not handle the heat generated by higher clock speeds (the "thermal wall") or support the power necessary to materially increase clock speeds with each new processor (the "power wall"). The last Netburst-based processor, Prescott, never clocked higher than 3.8 GHz. As a result, Intel scrapped Netburst and designed its next microarchitecture, known as "Core," to achieve higher performance through more efficient design.

120. Released in 2006, Core rejected Netburst's reliance on a deeply pipelined, single-core processor, in favor of dual- or multi-core processors with cache subsystems. Work on Core started in 2001, after Intel lost the speed crown to AMD and the initial failure of Netburst in the Willamette Pentium 4 processors.[23] Intel went back to its P6 microarchitecture design, and enlisted a team of engineers, who had designed the first microarchitecture for mobile computers (e.g., laptops), Pentium M, based on P6.[24]

121. Core-based processors relied on techniques, including OoOE, speculative execution, and branch prediction, to address stalls, misses, mispredictions, and other taxes on a processor's overall performance. On its release, Intel heralded Core as "a new foundation for Intel architecture-based desktop, mobile, and mainstream server multi-core processors," explaining that it had been "[d]esigned for efficiency and optimized performance across a range of market segments and power envelopes."

[23] "Key Nehalem Choices," Glenn Hinton Intel Fellow Nehalem Lead Architect Feb 17, 2010.

[24] https://www.tomshardware.com/reviews/Intel-i7-nehalem-cpu,2041.html (last visited Aug. 24, 2018).

122. With Core, Intel expanded its use of Dynamic Execution (OoOE, speculative execution, and branch prediction) to enable delivery of more instructions per clock cycle. Intel designed each "core" or independent processing unit within the processor, often called a "processing element" or a "core," such that it could fetch, dispatch, execute, and retire up to four full instructions simultaneously. Intel increased the instruction buffers (similar to the Reservation Station in the P6 design) for greater execution flexibility.

123. Intel also attempted to enhance the Branch Prediction Unit. According to Intel, "branch prediction" is among the processors' functions that have "the greatest leverage for improving overall performance" because of the penalty associated with recovering from an incorrectly predicted branch. As Intel explained, "more efficient branch prediction gives better efficiency *with no other changes to the machine.*"[25]

124. Additionally, Core featured a redesigned memory and cache subsystems. With "Smart Memory Access," Intel purported to improve the processor's performance by more effectively utilizing the current system of buffers and cores to hide latencies created by accessing main memory. Intel also imbued each execution core with the ability to speculatively load data for instructions prior to execution. With "Advanced Smart Cache," Intel created a large shared L2 cache accessible by both cores on a chip.

125. Intel's renewed reliance on Dynamic Execution, including branch prediction, and efficient memory and cache access led to reports of increased performance in processors based on the Core architecture. Core-based desktop and server processors boasted 40% and 80% increased

[25] "The Next Generation of Intel Core Microarchitecture," Intel Technology Journal, Volume 14, Issue 3 (2010). All quotes unless otherwise specified are from this source.

performance, respectively, over similar processors based on Netburst.[26] And these performance increases came at decreased clock speeds—the 2.66 GHz Core Duo 2 achieved 40% greater performance over a 3.6 GHz Netburst-based Pentium D processor.[27] With Core, Intel won back the performance crown[28] and stabilized its market share.[29]

8. "Tick/Tock" and the Nehalem Architecture

126. Beginning with Core, Intel made "[p]erformance . . . an integral part of production definition and success." To that end, "Intel set[] very aggressive performance targets to deliver products with compelling performance to the end user."[30] Intel also "employ[ed] significant time and effort to ensure that the processor performance me[t] expectations at every stage of the product development cycle from concept to silicon arrival to product launch. All design decisions [we]re weighed against performance impact."

127. With the introduction of Core in 2006, Intel announced "an ambitious plan to return to evolving its processor architectures at a rapid pace, as they had done in the mid-1990s" known as "Tick-Tock."[31] Each "Tick" represented Intel's effort to optimize the current microarchitecture design for a new manufacturing process or, in other words, shrinking the processor to fit on a smaller piece of silicon. The first "Tick" after Core was the Penryn microarchitecture, which

[26] 2006 Intel Annual Meeting Slides.

[27] Doweck, Jack, Inside Intel Core Microarchitecture, available at https://www.hotchips.org/wp-content/uploads/hc_archives/hc18/3_Tues/HC18.S9/HC18.S9T4.pdf (last visited Aug. 24, 2018).

[28] https://www.tomshardware.com/reviews/Intel-i7-nehalem-cpu,2041.html (last visited Aug. 24, 2018).

[29] 2006 Intel Annual Meeting Slides.

[30] "Original 45-nm Intel Core 2 Processor Performance," Intel Technology Journal, Volume 12, Issue 3 (2008).

[31] https://www.tomshardware.com/reviews/Intel-i7-nehalem-cpu,2041.html (last visited Aug. 24, 2018).

optimized Core for the 45 nanometers (nm) manufacturing process. Each "Tock" represented Intel's effort to redesign its microarchitecture. Under this product cycle, Intel utilized parallel design teams and committed to releasing either a Tick or a Tock each year.

128. The "starting point" for the first Tock following Core—known as Nehalem—was the previous Tick, the Penryn microarchitecture.[32] As Intel reported, with Penryn-based processors, "Intel delivered a product with record-breaking performance on a wide range of client and server applications" by implementing "[f]requency improvements," "a larger L2 cache," and other "microarchitectural enhancements."[33] With the Nehalem microarchitecture design Intel sought "a greater utilization of the possible peak performance" of the processor.

129. Work began on Nehalem in 2003. While most of the microarchitecture decisions were made in 2004, the major engineering work was done between 2005-2007.[34] Because Intel was forced to get Core out the door quickly to stop the fallout from Netburst, Core was not fully optimized for all types of processor use cases.[35] Whereas Core supported up to two cores, Nehalem was designed to effectively and efficiently support multiple cores and for use in laptops, desktops, and servers alike.[36] Or, as Intel told shareholders at its 2006 Annual Meeting, "One Micro-Architecture for all High Volume Segments."

[32] "The Next Generation of Intel Core Microarchitecture," Intel Technology Journal, Volume 14, Issue 3 (2010). All quotes unless otherwise specified are from this source.

[33] "Original 45-nm Intel Core 2 Processor Performance," Intel Technology Journal, Volume 12, Issue 3 (2008). All quotes in this section unless otherwise specified are from this source.

[34] "Key Nehalem Choices," Glenn Hinton Intel Fellow Nehalem Lead Architect Feb 17, 2010.

[35] https://www.tomshardware.com/reviews/Intel-i7-nehalem-cpu,2041.html (last visited Aug. 24, 2018).

[36] "Key Nehalem Choices," Glenn Hinton Intel Fellow Nehalem Lead Architect Feb 17, 2010.

130. To accomplish this, and eliminate a perceived "performance bottleneck," Intel implemented branch prediction in Nehalem's OoOE engine that sought to feed the engine "code and data at an unprecedented rate." As explained by *Ars Technica*, "to imagine that the [Penryn-based processor's] thirsty execution engine has been separated from the pools of code and data that lay in main memory by relatively thin pipes (the frontside-bus and cache hierarchy)" by "replacing the plumbing with very wide pipes and beefing up the pump in order to take full advantage of all this new capacity," Nehalem's design allows the processor to "get much closer to reaching its full potential."[37] Intel also enlarged the "out-of-order" window (e.g., where instructions are executed in dataflow order) by 33% and increased the size of the load, store, and reorder buffers in order to make room for more instructions form predicted branches.

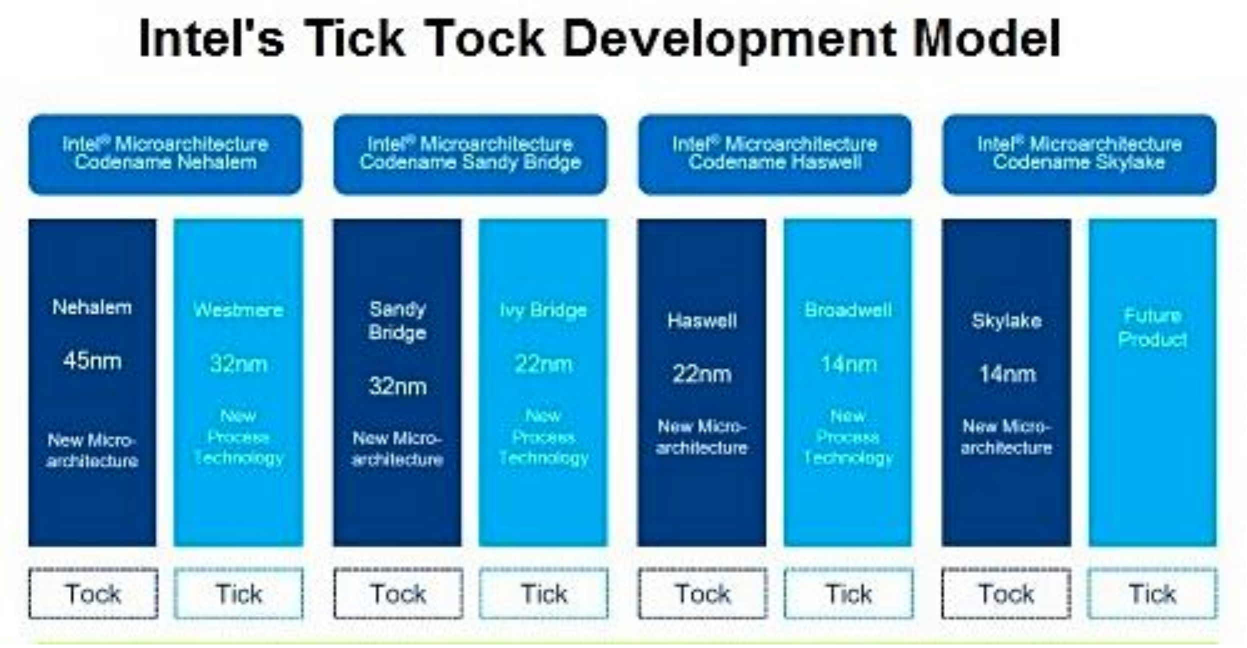
131. Intel also attempted to "deliver a per core performance increase" in Nehalem-based processors. To that end, Intel added a Level 3 or L3 cache that was shared between all of the processors' cores. In prior iterations of Intel's architecture, customers had "to choose between high-performance when all cores [were] active or high performance when only some cores [were] being used." "Having such a shared cache allow[ed] the entire cache to be used by any subset of the cores, in line with [Intel's] goal of not penalizing applications that cannot take advantage of all cores."

132. In addition to addressing per-core performance, Intel designed Nehalem to address the Company's shortcomings in the server space. For instance, Intel re-introduced "hyper-threading" technology in processors. A form of simultaneous multithreading technology, Intel's Hyper-Threading Technology or HT allows a CPU to duplicate certain of its resources virtually in

[37] https://arstechnica.com/gadgets/2008/04/what-you-need-to-know-about-nehalem/2/ (last visited Aug. 24, 2018).

order to increase the number of independent instructions in its pipeline. In the server space, HT allows a number of virtual machines to operate seamlessly (and separately) on the same physical server. Accordingly, Intel designed the Nehalem architecture to "further increase the utilization of the [architecture] design" and "to improve the throughput of the core for multi-threaded software environments."

133. Following the major advances of Core and the Nehalem architectures, Intel continued releasing either a Tick or Tock every 12-18 months until 2016 as follows:



134. With each Tock, Intel sought to enhance its Dynamic Execution (OoOE, speculative execution, and branch prediction) and cache subsystem in pursuit of increased performance of each successive processor. With each Tock, Intel implemented a new manufacturing process known as a process or die shrink. During a process shrink (e.g., moving from 45 nanometers ("nm") to 32 nm), the CPU, and in particular, its transistors, are scaled down to fit on a smaller piece of silicon.

135. A process shrink can make a CPU both more powerful and efficient. Smaller transistors mean that more transistors can be packed onto the die, increasing the available power. Less space between the transistors means that information can flow more efficiently, increasing the performance. However, the higher number and concentration of transistors also generates more heat. As a result, when Intel optimized its "Tick" microarchitecture for a new manufacturing process, Intel relied upon shared resources (e.g., shared L3 caches) in an attempt to balance power, efficiency, and thermal output in its processors, including, in particular, its multi-core processors.

136. In 2016, Intel retired "Tick/Tock" in favor of a new product cycle known as Process-Architecture-Optimization. Under the new product cycle, Sky Lake (formerly a Tock) is now an "Architecture" improvement, with the follow-on microarchitectures, Kaby Lake (2017) and Coffee Lake (2018), considered "Optimizations" of Sky Lake.

9. Intel's Claimed Focus on Security with Core Tick/Tocks

137. Beginning with Westmere, the "Tick" following Nehalem, and continuing with each successive Tick/Tock, Intel touted the security of its processors through its vPro offering, often with the tagline, "Secure to the Core."

138. Launched in 2007, vPro included Intel's Active Management Technology ("AMT") and a suite of security technologies for commercial uses of Intel processors including, among others, Intel Trusted Execution Technology ("TXT") and Intel Data Protection Technology (e.g., Intel Advanced Encryption Standards—New Instructions ("AES-NI")). In particular, in *Service Security and Compliance in the Cloud*, Intel Technical Journal, Volume 16, Issue 4, 2012 ("ITJ"), Intel recognized that "[s]ecurity is a key barrier to the broader adoption of cloud computing" (*id.* at 35), and that a fundamental security challenge facing cloud computing is the ability of an unauthorized user to launch a "side-channel" attack to extract information from VMs running on

the same system.[38] Intel described TXT as embedded hardware technology in its vPro chips to secure against such risks.

139. TXT is a "hardware-based" technology intended "to protect sensitive information from software-based attacks." To that end, TXT purportedly provided "[h]ardware-assisted methods that remove residual data at an improper [measured launch environment] shutdown, protecting data from memory-snooping software and reset attacks."[39] According to Intel, TXT "addresse[d] the increasing and evolving security threats across physical and virtual infrastructures" and was one of the "building blocks" through which Intel was "setting an industry benchmark for secure processing in data centers."[40]

140. Intel also intended TXT to allow for "[p]rotected execution," whereby an application can "run in [an] isolated environment so that no unauthorized software on the platform can observe or tamper with the operational information."[41] Based on these features, Intel described TXT as a key ingredient for building trusted platforms that allow IT administrators the ability to control virtualized or cloud-based machines able to withstand attacks, including (according to Intel) firmware, rootkit, and side-channel attacks.

141. AES-NI refers to new instructions that Intel developed to provide "hardware support" for the Advanced Encryption Standard. Adopted by the U.S. Government in 2001, AES

[38] In connection with its statements, Intel cited to "Ristenpart, T., Tromer, E., et al., *Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds*" CCS'09, Chicago, Illinois, in which the authors warn of the risks of side channel attacks in a VM environment. The authors further noted that these side channel attacks exploit time-shared caches "which appear to be particularly conducive to attacks." *Id.*, ¶ 8.5.

[39] Intel Trusted Execution Technology White Paper.

[40] Intel Trusted Execution Technology White Paper.

[41] "Service Security and Compliance in the Cloud," Intel Technology Journal, Vol. 16, Issue 4 (2012).

relies on cryptography to ensure the confidentiality of communications through an insecure or public/shared channel. However, cryptographic functions are traditionally seen as too complex and "computationally costly" to execute efficiently. As Intel explained in a 2010 white paper, "[i]t is expected that when encryption is turned on, performance will degrade." With AES-NI, Intel purportedly sought "to protect data" stored on hardware resources (e.g., processors) shared by several virtual machines in a data center from unauthorized access, use, or alteration through encryption, while removing "the main objection to using encryption to protect data: the performance penalty." In particular, Intel asserted that AES-NI "help[ed] prevent software side-channel attacks."

142. In launching "Haswell," the fourth generation of the Core microarchitecture, in 2014, Intel touted vPro's ability to "protect the OS kernel" from incursions. What Intel failed to disclose was that the privileged information typically stored within the OS kernel (or metadata sufficient to identify the privileged information) was not secure and could be leaked through side-channel attacks on the unsecured caches within Intel's processors.

143. With the launch of "Skylake," the sixth generation of the Core microarchitecture in 2015, Intel touted the CPUs' "cutting-edge security,"[42] claiming "[t]he Skylake architecture has been designed to enable better security"[43] not just for enterprise consumers through the vPro platform[44] but all consumers "at home." Intel asserted consumers were "safe and secure at home"

[42] https://www.intel.com/content/dam/www/public/us/en/documents/sales-briefs/modernize-with-6th-gen-core-vpro-brief.pdf (last visited Aug. 24, 2018).

[43] http://download.intel.com/newsroom/kits/core/6thgen/pdfs/6th_Gen_Intel_Core-Intel_Xeon_Factsheet.pdf (last visited Aug. 24, 2018).

[44] http://www.wcs.calculatedresearchandtechnology.marketingstudio.intel.com/sw/swchannel/CustomerCenter/documents/19765/39003/Powerful_to_the_Max_Secure_to_the_Core.pdf (last visited Aug. 24, 2018)

"knowing all of [their] pictures, videos, and personal files [were] securely stores at home." The "6th gen Intel Core processors with hardware-based security features help keep your system and data free from malware, hacking, viruses, and prying eyes."[45]

144. Intel represented to users that its CPUs were "secure to the core." Intel fully appreciated and recognized that many information security standards and regulations require "the protection of sensitive data" and asserted that Intel's processors "stand out" by "extending protection outside the operating system and into the hardware layer."[46]

145. Similarly, prior to January 2018, Intel recognized that cyber-attacks were "moving down the computing stack, traversing from software to hardware, threatening devices in homes, cars, businesses, networks and cloud," making it such that "[t]he legacy model of software protecting software can't keep up with advancing threats against digital security, safety and privacy." To address this, Intel designed "hardware-enabled security capabilities" directly into its processor, thereby allowing the CPU to protect the computing ecosystem "against evolving and modern threats."[47] Ultimately, while Intel touted its "leading edge security," Intel's decisions with respect to the implementation of speculative execution and its caches led the Company to be uniquely exposed to at least two major categories of exploits—Meltdown and Foreshadow.

[45] https://www.intel.com/content/www/us/en/desktops/desktop-storylines-security-infographic.html (last visited Aug. 24, 2018)

[46] https://www.intel.com/content/dam/www/public/us/en/documents/brochures/authenticate-product-brief-english.pdf (last visited Aug. 24, 2018)

[47] https://web.archive.org/web/20170407073442/https://www.intel.com/content/www/us/en/security/hardware/hardware-security-overview.html (last visited Aug. 24, 2018)

B. Intel's Processors Are Defective

1. Security Vulnerabilities Created by Intel's Use of Speculative Execution and an Unsecured Cache Subsystem Lead to Confidentiality Security Breaches

146. Ensuring the "confidentiality" of secret, sensitive, or private information by preventing its disclosure to an unauthorized entity is one of the most basic security properties, and an obligation Intel and its competitors in the industry acknowledged and accepted when designing new CPUs to release in the market. One way to protect the confidentiality of sensitive information is by controlling access to the information such that only authorized users can read or modify it.[48] Since 1985, Intel microarchitecture designs have relied upon protected mode and virtual memory to ensure that sensitive information is protected from unauthorized access

147. A "security attack" or exploit is a specific action that can cause a "security breach" or an event that violates a basic security property. It is characterized by a detailed description of the vulnerability exploited, the path of attack, and the subject of the attack. Critically, attacks that breach confidentiality are hard to recover from because once the information is disclosed, it is already too late.[49] A "security vulnerability" is a weakness in the system that can be exploited in a security attack.[50]

148. Unbeknownst to consumers, Intel sacrificed security for speed. Specifically, and as explained herein, Intel's implementation of Dynamic Execution created security vulnerabilities within its CPUs, rendering them defective. For example, Intel undermined the security of its processors by implementing OoOE and speculative execution in a way that (i) created windows of

[48] Security Basics for Computer Architects by Ruby B. Lee.

[49] Security Basics for Computer Architects by Ruby B. Lee.

[50] Security Basics for Computer Architects by Ruby B. Lee.

time during which an unauthorized user could have the processor make unnecessary or unauthorized memory accesses to copies of sensitive or privileged information and (ii) allowed that information (or critical data about the location or contours of that information) to remain in the CPUs' caches after the mistaken or unauthorized access (e.g., an exception) was discovered.

149. Intel likewise undermined the security of its processors by implementing a shared cache design that did not (i) include any mechanism to ensure that sensitive or privileged information (or data concerning that information) was flushed once the processor determined it had unnecessarily or improperly accessed memory, or (ii) provide any protection against side channel attacks that use the cache to siphon out data that remains in the cache after a processor completes its tasks.

150. As explained below, Intel knew that its processors, and in particular, the CPUs' cache subsystems, were vulnerable to side-channel attacks, and that side-channel attacks could be used to "leak" confidential information that was exposed as a result of Intel's implementation of OoOE and speculative execution in its CPUs.

2. Intel Knew That Its Architecture Was Susceptible to Side-Channel Attacks

151. Leaking information through covert or side-channels is one type of security attack that can lead to a confidentiality security breach. In a side-channel attack, a malicious actor exploits a security vulnerability to access or monitor information about the implementation of a computer system for the purpose of learning about or accessing otherwise privileged information. In this way, private information is deduced from observing the side-effects of operations. Such attacks need not depend on software bugs. Instead, as described here, they can exploit hardware vulnerabilities.

152. In a “timing” side-channel attack, a malicious actor exploits a security vulnerability with the express purpose of obtaining information about how long it takes the computer to complete a task, in order to infer something about otherwise privileged information. If someone can determine how long it takes a CPU to fetch instructions or data it needs to complete its operations, he can infer where the information is located within the system, and, ultimately, the substance of the information.

153. In particular, it takes less time to access data that resides in a processor’s cache subsystem than data that must be retrieved from main memory. By measuring the amount of time it takes for a processor to fetch instructions or data, an attacker can learn whether the requested information is in the cache or in main memory. If certain data is stored within the cache subsystem or “cached,” an attacker can deduce that it has been accessed recently. Once an attacker has access to these measurable differences in the amount of time it takes to access different kinds of information, he can work backwards to discover the underlying information.

154. Consider the following analogy. An individual (e.g., the attacker) goes to a library (e.g., the computer) to read a book (e.g., data) from a special collection the individual does not have permission to access (e.g., kernel memory). The individual asks the librarian to retrieve “Special Book #1 and the Sue Grafton novel that corresponds to the first letter of page 1 of Special Book #1,” (e.g., a program instruction). The librarian retrieves (e.g., fetches) Special Book #1 from the special collection and determines (e.g., decodes) that the first letter on page 1 of that book is “C,” requiring the librarian to also retrieve “C is for Corpse,” by Sue Grafton. The librarian returns to the front desk with Special Book #1 and “C is for Corpse” by Sue Grafton. Before the librarian shows the individual the requested books, she checks his library card. If the librarian determines that the individual does not have permission to access books in the special collection,

she will put the books on a cart to be re-shelved (e.g., the cache) without showing them to the individual.

155. Knowing that the Sue Grafton book with the title corresponding to the first letter on the first page of Special Book #1—the book the individual wants to read but does not have permission to access—is now on the cart, the individual begins methodically requesting Sue Grafton books, starting with "A is for Alibi." If the librarian responds to this request with "please wait while I go and retrieve that book," the individual knows that book is not on the re-shelving cart and the first letter on the first page of Special Book #1 is not A.

156. However, when the individual requests "C is for Corpse," the fact that the librarian is able to quickly retrieve it from the re-shelving cart reveals to the individual that the first letter on page 1 of the Secret Book #1 is "C." If it takes nanoseconds to complete these tasks (as it would within a CPU), the individual could determine fairly quickly the contents of Special Book #1 without ever actually seeing the book itself. In the same way, a timing side-channel attack on a CPU cache allows a malicious actor to gather enough data about where sensitive or privileged information is located within the computer to deduce the precise contours of that sensitive or privileged information.

157. Although unknown to the public, the susceptibility of Intel's cache design to side-channel attacks was described by technical researchers concerning early iterations of its processors. In fact, discussions of the fundamental problems that underlie the vulnerabilities appear in literature from the early- to mid-1990s. For example, Sibert, *et al.*, *The Intel 80x86 Processor Architecture: Pitfalls for Secure Systems* (1995), identified exploitable weaknesses in Intel's microarchitecture and explained that caches may be used as covert timing channels to leak sensitive information. *Id.*, § 3.10 (citing Wray, *An Analysis of Covert Timing Channels* (1991)).

The authors emphasized that the imbalance in scrutiny of hardware security had already become "untenable" and "increasingly difficult to justify." Sibert, §§ 1, 2.[51] Intel's design response and associated micro-architectural changes to address these and other expressed security concerns have been largely confidential.

158. In a 2010 white paper entitled, *Securing the Enterprise with Intel AES-NI* (2010), Intel described an on-going problem with AES cryptographic keys, noting that "in multiple processing environments . . . a piece of malicious code running on the platform could seed the cache, run cryptographic operations, then time specially crafted memory accesses to identify changes in the cache. From these changes, the attacker could determine portions of the cryptographic key value" which can then be used to defeat AES encryption. To solve this problem, Intel launched AES-NI, *see supra*, which protected AES cryptographic keys from side-channel attacks by ensuring that this information was never stored in the CPU's caches. However, despite knowing that the root cause of the side-channel attack against AES was an attacker's ability to "seed the cache" and "identify changes in the cache," Intel did not secure the cache subsystem from side-channel attacks. So, though Intel implemented AES-NI to help avert cache timing side-channel attacks against AES by eliminating the use of cache for AES calculations, Intel did nothing to address the fundamental flaw in its leaky cache design.

159. The vulnerability created by Intel's decision to leave the cache subsystem unsecured is exacerbated when the cache is shared among the CPU's threads and cores. For over

[51] *See also* Paul C. Kocher, *Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems*. Advances in Cryptology—CRYPTO, Vol. 1109 Lecture Notes in Computer Science, 104-113 (1996) (a seminal work on timing attacks, which noted the potential to exploit timing measurements from vulnerable systems to find entire secret keys, and specifically referenced RAM cache hits as a source of such exploitable timing differentials).

a decade, Intel knew, or reasonably should have known, that unauthorized users could exploit a CPU resource (such as a cache or buffer) that is shared by two processes running simultaneously on the CPU. In effect, one process may "spy" on the other by examining changes made to that shared resource by the other process.

160. Computer security researcher Colin Percival demonstrated one attack of this kind in late 2004. Percival showed that on Intel CPUs with a "Hyper-Threading" design, where multiple threads (i.e., processes) are scheduled to run simultaneously on the same processor, the use of shared memory caches allowed a malicious process to make deductions about the other program's behavior and steal information, in this case, cryptographic keys. Percival described having caches shared between threads as a vastly dangerous avenue of attack. He notified Intel of this problem in early 2005, prior to presenting his paper describing the attack, *Cache Missing for Fun and Profit* (2005).[52] At approximately the same time, another group of researchers published a work that similarly showed exploitation of the shared cache through two techniques.[53]

161. The attack Percival detailed is one variation of the same basic theme—an unauthorized actor exploiting the changes a process causes to the micro-architectural state of a CPU (in particular, a shared memory cache) in order to acquire another's information. In fact, any time a resource is shared, there is a possibility information can leak. For example, if one CPU

[52] *See* http://www.daemonology.net/blog/2018-01-17-some-thoughts-on-spectre-and-meltdown.html (last visited July 26, 2018); *see also* http://www.daemonology.net/hyperthreading-considered-harmful/ (last visited Aug. 2, 2018).

[53] In Osvik, *et al.*, *Cache Attacks and Countermeasures: the Case of AES* (2005), the group explained that attackers could mount a powerful attack by determining which cache sets had been accessed by a victim program. First, in an attack known as Evict + Time, and attacker measures how execution time is influenced by evicting a chosen cache set to see whether a particular cache set was used by a victim. Second, in a Prime + Probe attack, the attacker can get better accuracy by measuring cache access times directly rather than indirectly through execution time.

core asks whether certain data is present in the L3 cache, the answer, a binary yes or no, provides some useful information about the current work the CPU is engaged in. If an unauthorized actor can access that information and analyze it, it could lead the actor directly to secret or privileged information thought to be protected in other parts of the computer.

162. In a 2006 paper, *Covert and Side Channels Due to Processor Architecture*, Dr. Ruby Lee and Zhenghong Wang, examining a different Intel processor family, presciently highlighted a new "speculation-based covert channel," arising from the fact that when Intel allows a load instruction to execute speculatively in the IA-64, although a bit is set in the register if the speculative load instruction would cause an exception, the exception is not handled right away. Instead, "[c]ontrol speculation allows deferral of the exception," including exceptions such as access violations, thereby opening the door for attackers to leak information via a side-channel attack. *Id.*, § 3.4.

163. Dr. Lee has emphasized that software-based solutions still left the "crown jewels of primary key material" susceptible to attack and that "[a]ll current processors with caches are vulnerable—from embedded devices to cloud servers."[54] In a paper published in 2007, in which Lee and Wang discuss thwarting side-channel attacks at the root, the authors cautioned that "[c]ache-based side channel attacks can be very dangerous" and "very effective." Wang, *et al.*, *New cache Designs for Thwarting Software Cache-based Side Channel Attacks* (2007), § 7.

164. At approximately the same time that Dr. Lee's paper was published, an analogous side-channel attack that exploited speculative execution and a shared CPU resource called the Branch Target Buffer (BTB), used in branch prediction, was described. *See* Acıiçmez, *et al.*,

[54] *See* https://www.hotchips.org/wp-content/uploads/hc_archives/hc26/HC26-10-tutorial-epub/HC26.10-tutorial1-HW-Security-epub/HC26.10.155-6_Lee_UniversityResearch_go.pdf (last visited Aug. 24, 2018).

Predicting Secret Keys via Branch Prediction (2006). Using the described exploit, an unauthorized actor could determine private cryptographic keys used in the target user's computer.

165. Later, in 2013, Yuval Yoram demonstrated a cache-based side-channel attack that showed that the attacker and victim process need not share the execution core. *See* Yoram, *et al.*, *Flush+Reload: A High Resolution, Low Noise, L3 Cache Side-Channel Attack* (2013). In this cross-core attack, as long as the processes had shared use of the cache, the attacker could identify the target's access to specific memory.[55] The crux of the attack is a weakness in Intel's X86 architecture; specifically, the lack of permission checks before permitting use of an instruction that allows an attacker to evict specific memory lines from cache. As the researchers observed, "Not restricting the use of the instruction is a security weakness of the Intel implementation of the X86 architecture," which "requires a hardware fix."[56] The authors cautioned that, "Given the strength of the attack, we believe that the memory saved by sharing pages in a virtualized environment does not justify the breach in the isolation between guests."

166. That same year, researchers described a side-channel attack for deducing information about privileged address space layout which can be used to defeat a common memory management security technique called kernel address-space-layout randomization ("KASLR").[57] Those attacks against Intel x86-based processors (specifically, Intel i7-870, Intel i7-950, and Intel i7-2600) are enabled because "hardware (such as caches and physical memory) are *shared* between

[55] This could be accomplished through a "Flush + Reload" technique in which (1) the attacker flushes a memory line from the cache, then (2) waits to give the victim an opportunity to access the memory line, and then (3) the attacker reloads the memory line, which will be quick if the victim did in fact access the line (since it is now back in cache) or will be significantly longer if the victim did not access the line, which then needs to be brought in from main memory.

[56] The authors note that ARM architecture also includes an instruction to evict cache lines but that it can only be used when the processor is in an elevated privilege mode.

[57] *See* Hund, *et al.*, *Practical Timing Side Channel Attacks Against Kernel Space ASLR* (2013).

privileged and non-privileged code" and "the nature of the cache facilities still enables an attacker to indirectly measure certain side-effects." Hund at 195 (emphasis in original).

167. By 2015, Intel knew, or reasonably should have known, that an attacker could mount a cache side-channel without the need to install code on a victim's machine. In Oren, *et al.*, *The Spy in the Sandbox: Practical cache Attacks in Javascript and their Implication* (2015), the authors described a cache side-channel attack that ran entirely in a web browser. Thus, "the victim needs only to browse to an untrusted webpage that contains attacker-controlled content" to facilitate an attack. *Id*. at Abstract.[58]

168. Thus, more than a decade of research papers describe cache side-channel attacks that exploit Intel's cache memory design to gain access to kernel memory and other privileged information.

169. Moreover, while Intel hid from the general consuming public that these vulnerabilities pose a severe security threat, in various patent filings Intel acknowledged the security risks caused by cache side-channel timing attacks. Intel was aware that its hardware design could be used to leak privileged information, and even claimed knowledge and awareness of means to modify its chip designs to prevent such attacks. *See Mitigating Branch Prediction and Other Timing Based Side Channel Attacks,* U.S. Patent No. 8,869,294 B2 (filed Dec. 5, 2007) (the "'294 patent") ("New mitigations to side channel attacks are needed to deter attempts to subvert the security of a computer system.") col. 1, lines 45-46; *Protecting Private Data From Cache Attacks*, U.S. Patent No. 8,516,201 (Dec. 5, 2007) (the "'201 patent") ("Cache-based side channel attacks have recently become a concern for applications that perform cryptographic

[58] Using their Javascript-based cache side channel attack, the authors were able to map more that 50% of a victim's cache in as little as one minute and gain access to the victim's mouse movements and network activity (i.e., websites visited).

operations . . . . Side channel attacks are also possible when two applications share the same cache.") col. 1, line 63-col. 2, line 5; *Protected Cache Architecture and Secure Programming Paradigm to Protect Applications*, U.S. Patent No. 8,341,356 B2 (filed May 3, 2011)[59] (the "'356 patent") (proposed invention "to prevent a so-called side channel attack in which an attacker program and a victim program . . . both use the same physical cache.") col. 2, lines 5-8; *Obscuring Memory Access Patterns in Conjunction with Deadlock Detection or Avoidance*, U.S. Patent No. 8,407,425 B2 (filed Dec. 28, 2007) (the "'425 Patent") ("side-channel attacks exploit aspects of multi-threading environments where two concurrent threads share computing resources" and "[o]ther exploits that use this type of information leakage may be readily envisioned") col. 1, lines 18-26.

170. As such, Intel's CPUs are materially defective. When Intel's processors engaged in speculative execution, the processors made information, which should have remained secure and inaccessible to unauthorized use, accessible in the processors' unsecured cache subsystem. In so doing, Intel's processors created a vast security vulnerability that could be accessed through a number of different exploits.

3. Intel Knew That Permitting Unprotected Memory Access During Speculative Execution Could Be Exploited by Side-Channel Attacks

171. Intel's implementation of speculative execution in its processors created a window of time during which an attacker could make unnecessary or unauthorized requests to access memory for information. As explained above, when a processor engages in speculative execution it fetches information it needs to execute instructions out of program order, allowing the CPU to avoid performance penalties when it encounters data dependent or conditional instructions. These

[59] The provisional application No. 60/873,051 was filed Dec. 5, 2006.

requests could be legitimate, e.g., the application requested access to information that is not itself privileged, but unnecessary, e.g., the information ultimately will not be utilized by the processor. These requests also could be illegitimate—e.g., the application requesting access to privileged information is not authorized to do so. Irrespective of the necessity or legitimacy of the request to access memory, the information fetched from memory was stored in the CPU's caches and buffers—a kind of cache that assists the processor in transporting information from one process to another—until it was needed.

172. Intel designed its processors to avoid taking any action to address unauthorized (e.g., exceptions) or unnecessary (e.g., mistakes) memory requests until such time as the processor was ready to retire the instructions in program order. This allowed the CPU to defer action on any mistakes or exceptions encountered during out-of-order or speculative execution until the end of the process to enhance the processor's performance. Intel's decision to defer these actions, however, allowed, without permission, sensitive or privileged information (or data about that information) to be transferred to and maintained in the CPU's caches or buffers.

173. A window created by Intel's implementation of out-of-order or speculative execution remained open until the instruction necessitating out-of-order or speculative execution in the first instance was complete—e.g., in the case of a conditional instruction (if X, then Y), when the CPU determines the correct branch direction and target. It was only after the window closed that Intel's processors addressed any mistakes (e.g., a mis-predicted branch where the memory access was legitimate but unnecessary) or exceptions (e.g., an application accessing data with insufficient privileges) that occurred while the CPU was engaged in out-of-order or speculative execution, and then flushed its pipelines of any impact from the related instructions.

174. However, the information fetched for instructions executed out-of-order or speculatively remained behind in the CPU's caches and buffers. In other words, while Intel's processors should have rolled back any impacts of executing unnecessary or improper instructions on the computer, Intel allowed the raw materials the CPU fetched to execute these instructions to remain in the processors' caches or buffers, and thus vulnerable to unauthorized access.

175. Intel relied on speculative execution to increase the performance of its processors even though it knew that, as Dr. Lee and her co-author, Wang, explicitly warned as early as 2006, that the deferral of exceptions "can be exploited to facilitate information leakage."[60] Six years later, Wang again warned of the risks of speculation-based side-channel attacks in his doctoral thesis, *Information Leakage Due to Cache and Processor Architectures* (Nov. 2012), on which Dr. Lee was the advisor, stating, "[w]e wish to emphasize the severity of this channel before real damage is done." *Id.* at 81.

176. Intel likewise knew through at least two other instances that the Company's decision to permit unchecked memory accesses in its processors presented a serious security vulnerability, exploitable by attackers siphoning information out of the processor cache through a side-channel attack—the "Prefetch Side Channel Attack" and the "TSX Side Channel Attack."

177. **Prefetch Side Channel Attack.** Intel's processors include a function known as "prefetch," with which a software program can direct the CPU to fetch data before it is needed. According to Intel, the prefetch instruction "can hide the latency of data access in performance-critical sections of application code by allowing data to be fetched in advance of actual usage." Because prefetch "merely provides a hint to the hardware," its usage "***generally does not generate exceptions or faults***" in the CPU. However, as explained in *Prefetch Side-Channel Attacks:*

[60] Wang, *et al.*, *Covert and Side Channels due to Processor Architecture* (2006).

Bypassing SMAP and Kernel ASLR (2016), "[p]refetch instructions on Intel CPUs ***ignore*** privilege levels and access permissions" making it possible for any attacker to use prefetch to access "inaccessible kernel memory" and then execute a cache-based timing side-channel attack to access the data put in the cache by the prefetch function. *Id.* § 3.2. The authors of *Prefetch Side-Channel Attacks* noted that Intel reference manuals from 2014 (and, indeed, by as early as 2012) reflect that the "prefetch" command could be used to access illegal or unprivileged memory space without generating any exceptions.

178. **TSX Side-Channel Attack.** In 2016, researchers revealed a timing side-channel attack that exploited an Intel hardware feature called Transactional Synchronization Extension (TSX). As researchers explained:

> One surprising behavior of TSX, which is essentially the root cause of this security loophole, is that it aborts a transaction without notifying the underlying kernel even when the transaction fails due to a critical error, such as a page fault or an access violation, which traditionally requires kernel intervention.

Jang, *et al.*, *Breaking Kernel Address Space Layout Randomization with Intel TSX* (Oct. 2016) ("Jang") at 380.

179. In other words, with TSX, the processor allowed a thread to perform a sequence of operations inside a transaction and if an exception due to unprivileged access occurs, the OS will not be notified. Instead, the exception will be suppressed, meaning, as stated in Intel's September 2016 manual, transactional execution would abort and it will be as though the exception or fault had never occurred. *See* https://www.intel.com/content/dam/www/public/us/en/documents/manuals/64-ia-32-architectures-software-developers-manual.pdf. The authors noted that because TSX suppresses exceptions, such as an access violation that is caused by accessing kernel space from a user process, TSX "exposes a clear, stable timing channel." Jang at 382. Jang goes on to describe a side-channel attack exploiting the suppression of exceptions by TSX that can "extract

the executable and non-executable bit of every kernel page and defeats KASLR ("Kernel Address Space Layout Randomization"). *Id*. Thus, the TSX side-channel attack, like the Prefetch Side-Channel Attack, is another instance in which Intel's suppression of exceptions was exploited by a timing side-channel attack to gain access to kernel information.

180. Intel knew, or should have known, that just as its suppression of exceptions under Prefetch and TSX could be exploited by a timing side-channel attack, the decision to defer taking action on memory access violations under speculative execution could also be exploited by side-channel attacks. This is precisely what occurred in Meltdown, Foreshadow, and Spectre.

4. "Meltdown"

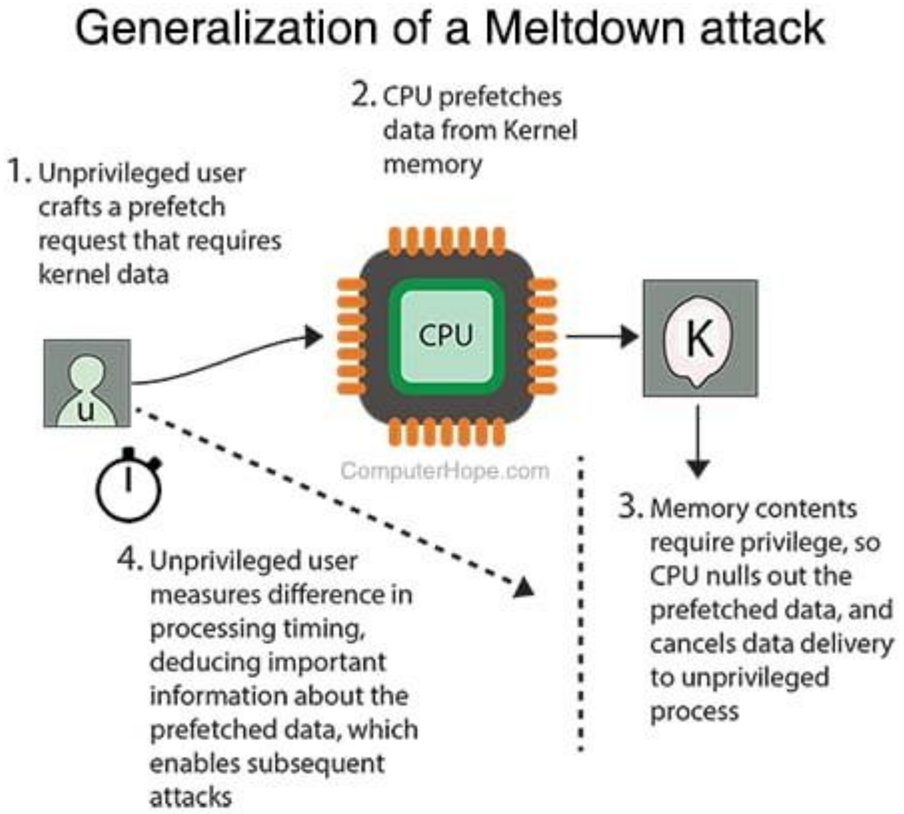
181. In July 2017, researchers identified "Meltdown" or "Rogue data cache load" (CVE-2017-5754), [61] also known as "Variant 3," and informed Intel. The attack has been nicknamed "Meltdown" by researchers due to its ability to effectively dissolve the informational barrier that protects privileged data, allowing an attacker to read sensitive information like passwords, login keys, and encryption keys.

182. Meltdown takes advantage of the fact that Intel CPUs use speculative execution to fetch data ***before*** enforcing a privilege check to confirm that the user is authorized to read such data. This is done to make Intel chips faster. If it turns out that the user attempting to access the data possesses the appropriate privilege level, allowing access to the data "speculatively" (i.e., without first checking and enforcing access permissions), saves time. If it turns out that the user lacked the appropriate privilege level, an error or "exception" occurs and the user should be denied

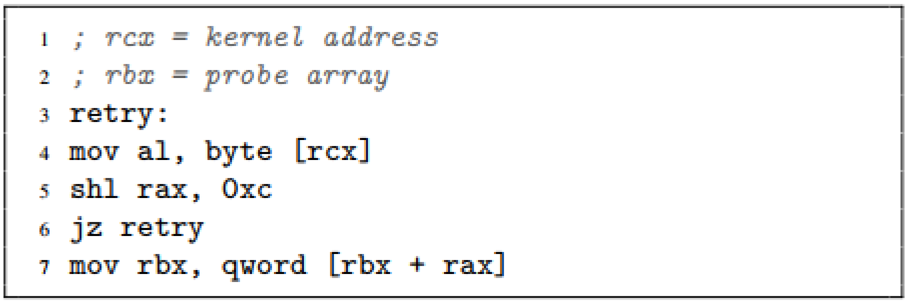
[61] CVE refers to Common Vulnerabilities and Exposures, a standardized, industry-endorsed list of security vulnerabilities.

access to the privileged data. Intel, however, defers enforcement of the exception thereby creating a window of time where a malicious actor can gain unauthorized access to privileged information.

183. By engineering a system that permits access to privileged information in a manner that allows a user to win a "race condition" between the instruction execution and the enforcement of a privilege check, the attacker can then deploy a side-channel attack to infer the privileged information from data contained in the cache after the exception was belatedly enforced, thereby rendering the privilege check useless. This is Meltdown in a nutshell.

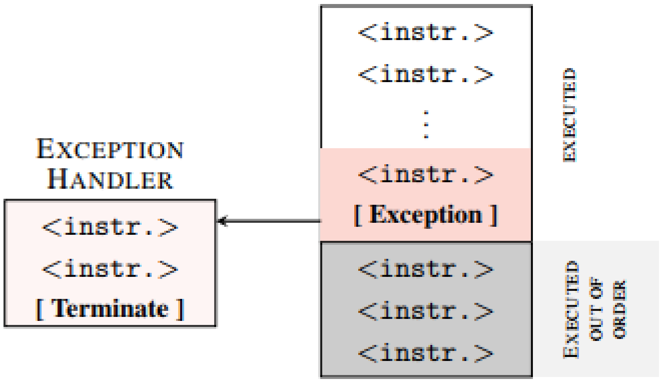

Generalization of a Meltdown attack
2. CPU prefetches data from Kernel memory
1. Unprivileged user crafts a prefetch request that requires kernel data
CPU
K
u
ComputerHope.com
3. Memory contents require privilege, so CPU nulls out the prefetched data, and cancels data delivery to unprivileged process
4. Unprivileged user measures difference in processing timing, deducing important information about the prefetched data, which enables subsequent attacks

184. The first step in a Meltdown attack is to run instructions that attempt to load the cache with an address that the attacker has rights to and that depends on secret data, which ordinarily triggers an exception:



```
; rcx = kernel address
; rbx = probe array
retry:
mov al, byte [rcx]
shl rax, 0xc
jz retry
mov rbx, qword [rbx + rax]
```

185. Because of speculative execution, the subsequent instructions to move the inaccessible address are executed speculatively and out of order, before the exception is handled, thereby loading the secret value into the cache without enforcing the privilege check on the user:



186. In order to ensure that all of the necessary instructions to complete the attack are speculatively executed before the exception is triggered, a Meltdown attack may exploit "exception handling" or "exception suppression" techniques that prevent the OS from terminating the program as soon as the exception is triggered. Once the exception is handled, the program is terminated, but the cache that now contains the secret data is not flushed.

187. Finally, a Meltdown attack uses a side-channel attack, such as "Flush+Reload," to repeatedly probe the contents of the cache by flushing and reloading its contents while monitoring small differences in the time it takes to access the loaded cache block. Through this process, an attacker can determine where in the cache the privileged memory was stored and deduce the contents of that memory. For example, assuming the secret data is the value "15," the attacker

will probe cache blocks 1-15. If the timing differences in flushing and reloading the cache indicate that block 15 is present, the attacker can infer that the secret data is 15.

188. By repeating these steps, an attacker can read not only "kernel" memory, which is the most protected memory on a computer, but because all major operating systems also typically map the entire physical memory into the kernel address space, an attacker can also read the entire physical memory of the target machine.[62] The result is that a bad actor can entirely bypass the privilege-mode isolation on a machine to access its most sensitive and confidential information, like secret passwords, without detection.

189. Meltdown is believed to affect virtually all out-of-order Intel processors released since 1995.

190. Meltdown is extremely similar to the Prefetch Side-Channel Attack. For instance, both the Meltdown and Prefetch Side-Channel Attack "melt down" the boundary between user space and kernel space and exploit Intel's failure to enforce privilege checks and access permissions prior to granting access to kernel memory. Additionally, the team that discovered Meltdown used the exception suppression "feature" of TSX to carry out their Meltdown attack. *See* Lipp, *et al.*, *Meltdown*, at 6.

191. Significantly, because of differences in AMD's (and other competitors') architecture and implementation of speculative execution, their CPUs are not vulnerable to

[62] Kernel memory addresses are mapped in the user process's virtual address space and corresponding page table (along with the user's own virtual memory addresses). This is done so that when a switch into kernel mode is required, *e.g.*, because of either a system call (*i.e.*, asking OS to do something) or an interrupt happens, the switch to kernel mode can be done quickly since the kernel addresses are already mapped in the page table for the user's address space. Kernel memory address ranges are marked as non-accessible so that the user program itself cannot read or write to those spaces of kernel memory. Unfortunately, as Meltdown demonstrates, Intel CPUs speculate past those protections, making that data obtainable by unauthorized actors.

Meltdown side-channel attacks. This is an issue residing solely with Intel and based on Intel's misplaced design decisions.

5. "Foreshadow" or "L1 Terminal Fault"

192. In January 2018, a group of researchers discovered another attack that exploits Intel's implementation of speculative execution. After the first variant (which targeted Intel's SGX technology) was identified, Intel's subsequent investigation uncovered two closely related attack variants. The first variant has been dubbed "Foreshadow," and the later two variants have been dubbed "Foreshadow-NG" (for "Next Generation") by researchers; Intel refers to the attacks collectively as L1 Terminal Fault (or L1TF). Like Meltdown, the Foreshadow attacks are based on the fact that Intel's hardware speculates past permission checks, allowing a malicious process a window of time during which it can steal sensitive information.

193. **Relevant Computer Architecture Background.** The L1 (level 1) data cache is a memory resource shared between all software running on the same core. Therefore, the ability to speculatively access data left in the L1 cache can have serious security consequences. Even worse, modern Intel processors with Hyper-Threading also share the L1 cache between sibling cores.

194. Generally, and as discussed previously, to achieve a secure computer system each process has its own separate virtual address space. When a process accesses a memory location in its virtual address space, the hardware translates the address into the corresponding physical address. One process should not be able to access another process' physical address space (unless the two processes are explicitly sharing data, *e.g.*, to communicate with one another). Software keeps track of data access permissions by mapping virtual to physical addresses through page tables. The page tables are used to translate each process's virtual addresses to the physical addresses corresponding to its memory locations.

195. During a page table check or "walk" the processor will perform the translation and will also check whether the page is actually "present" in main memory. Non-present entries can exist when a virtual page that has not been used recently is "swapped" or moved out to disk and the corresponding page table entry is then marked to show that process's page is not present. When access to that absent memory location is requested, a page fault (a kind of exception) will occur, the address translation process will terminate, and the missing data must be located on disk, and pulled back into physical memory.

196. But to speed performance, in the meantime Intel CPUs will continue to speculate forward. Modern Intel CPUs are designed so that if the address translation process is prematurely terminated through a page fault, the L1 cache lookup is still performed based on the physical address pointed to in the page table (which is no longer the physical memory of the requesting process), and speculative instructions are temporarily permitted to perform computations using secret data that the process is unauthorized to access from the cache. The Foreshadow attacks are also referred to as "L1 terminal fault" because they cause the translation process to prematurely terminate through a page fault, while, dangerously, data is still being passed from the L1 cache to subsequent instructions.

197. Finally, as in the Meltdown attack, attackers can use the "Flush+Reload" technique to establish the secret information.

198. **Foreshadow-OS (CVE-2018-3620).** This variant allows an unprivileged application to access kernel memory. A malicious application can simply wait for the OS to clear the "present" bit in a page table entry (which happens when a memory page that has not been used recently is swapped out of memory to disk). The malicious actor inputs a virtual address, which must be translated through the page table. Since the bit is marked not present in the page table,

the translation process is terminated. Because of Intel's implementation of speculative execution, the malicious actor can use speculative instructions to read any cached contents pointed to by the physical address from the page table entry.

199. **Foreshadow-VMM (CVE-2018-3646).** The mapping and translation process is modified slightly in a "virtualized" environment, where multiple guest operating systems run on the same machine, as in cloud computing. The Foreshadow-VMM variant allows a malicious guest virtual machine to access memory belonging to other guest virtual machines and the hypervisor (which is the software that manages the virtualized environment).

200. In a virtualized environment, two translations may occur by using "extended" page tables. First, the guest machine's virtual address is translated to a guest "physical" address through its guest page table. Second, the guest "physical" address is translated to the underlying machine's host-physical address using the host page table.

201. A malicious guest has control over the guest page table and therefore can directly clear the "present" bit in that page table. That triggers the page fault, which terminates the translation process, eliminating the host address translation step. Due to Intel's flawed implementation, it is the guest "physical" address that is passed to the L1 data cache. Notably, because in this variant the guest has control over the guest page table and thus controls the "physical" address, the malicious guest can speculatively read any cached memory, including secret data belonging to other virtual machines or the hypervisor itself.[63]

[63] Whereas the Meltdown attack described above was limited to reading privileged supervisor data mapped within an attacker's virtual address space, the Foreshadow-type attacks directly expose cached physical memory contents to malicious actors from locations that are not mapped in the attacker's physical address space.

202. **Foreshadow-SGX (CVE-2018-3615).** Intel's Software Guard eXtensions ("SGX"), introduced in 2013, allow users to allocate private regions of memory called "enclaves," which are intended to allow secure execution on an adversary-controlled machine. With SGX, an additional level of checks is supposed to be performed after the address translation process is completed in order to enforce strict access control for enclaves. In the SGX variant, attackers can exploit the L1TF behavior described above to terminate the address translation process so that any cached enclave secrets are passed to speculative out-of-order execution before SGX protections are enforced. Additionally, as with Meltdown, attackers can leverage the TSX exception suppression "feature" to carry out the attack.

203. Ironically, while Intel stated that SGX was "designed to increase the security of application code and data," *see* https://software.intel.com/en-us/sgx, SGX is itself vulnerable to the Foreshadow side-channel attacks. *See* https://arxiv.org/pdf/1709.09917.pdf.

204. Like the Meltdown vulnerability, AMD's and other competitors' CPUs are not vulnerable to Foreshadow side-channel attacks. Foreshadow is exclusively an Intel CPU problem and the result of Intel's improper implementation of speculative execution.

6. "Spectre"

205. Beginning in April 2017, researchers discovered the first in a series of related security attacks or exploits known as Spectre. Spectre gets its name from "speculative execution." Intel was aware of the first two Spectre variants by June 1, 2017. The public did not become aware of Spectre or the security vulnerability it exploited until January 3, 2018.

206. Generally speaking, a Spectre attack takes advantage of the security vulnerabilities created by Intel's reliance upon speculative execution, and in particular, the branch prediction unit, and an unsecured cache subsystem to achieve increased performance. Critically, it is difficult to

detect the execution of a Spectre exploit in part because the CPU does not recognize that its "mis-speculation" was, in fact, coerced, and cache-timing side-channel attacks generally leave no readily discernible trail to indicate that the caches have been improperly accessed. Thus, the attacker can compromise the CPU and obtain sensitive information without leaving any fingerprints behind.

207. Each Spectre exploit involves several steps. First, the attacker uses a "leak gadget" to coerce the CPU to speculatively execute instructions that are not a normal part of the processor's operation. Second, unware that it is under attack, the CPU fetches and stores within its caches the data needed to execute the coerced instructions. Third, still unaware that it is under attack, the CPU determines that it has "mis-speculated," or speculatively executed incorrect instructions, and proceeds to flush its pipelines—but not its caches—of the effects of the incorrect instructions. Finally, the attacker uses a "transmit gadget" to execute a side-channel attack on the CPU's caches and surreptitiously transmit the information that remains after the processor's mis-speculation. By July 10, 2018, researchers had identified six Spectre variants as follows:

Name of Variant	**Date 1st Identified**	**Date 1st Released**	**Key Attributes of Variant**
Variant 1, Bounds Check Bypass (CVE-2017-5753)	June 2017	1/3/2018	Exploits the speculative operations that occur when CPUs execute certain conditional branch instruction—e.g., whether an input is "in bounds"—to engage in otherwise unauthorized or unnecessary memory accesses.

Name of Variant	**Date 1st Identified**	**Date 1st Released**	**Key Attributes of Variant**
Variant 1.1, Bounds Check Bypass on Loads (CVE-2018-3693)		7/10/2018	Exploits speculative stores and how the CPU addresses speculative buffer overflows to bypass mitigations implemented for earlier Spectre variants. This variant uses a form of "stack smashing," a common method of capitalizing on a buffer overflow.
Variant 1.2, Read-only Protection Bypass		7/10/2018	Exploits speculative stores and how the CPU addresses speculative buffer overflows where the processor doesn't enforce read/write protections to bypass mitigations implemented for earlier Spectre variants.
Variant 2, Branch Target Injection (CVE-2017-5715)	June 2017	1/3/2018	Exploits the part of the CPU that directs what operations need to be speculatively executed (the "indirect branch predictor") to allow malicious code to be speculatively executed.
Variant 3a, Rogue System Register Read (CVE-2018-3640)		5/23/2018	Exploits the "read system register" function to allow an attacker to improperly access information about the state of the CPU's system register (similar to a cache).
Variant 4, Speculative Store Bypass (CVE-2018-3639)		5/23/2018	Exploits the CPU's ability to speculatively load data into its caches.

208. On July 23, 2018, a team of security experts from the University of California, Riverside disclosed a new Spectre attack, SpectreRSB.[64] In a SpectreRSB exploit, an attacker exploits a different component of the microarchitecture utilized in speculative execution—the return stack buffer or RSB. The purpose of an RSB in a processor employing speculative execution

[64] https://arxiv.org/pdf/1807.07940.pdf (last visited Aug. 24, 2018).

is to predict where a CPU should go to, or the "return address," once its current operation is complete. Like the other variants of Spectre, SpectreRSB involves utilizing a "leak gadget" to poison the RSB, which has the effect of either mis-training or polluting the branch prediction unit to force it to speculatively execute certain instructions.

C. **Intel Was Aware of Numerous Methods That Would Have Mitigated Cache Side-Channel Attacks**

209. As many of its patent filings show, Intel was fully aware of the vulnerability of its architecture to cache side-channel attacks and the steps it could have taken to plug the security holes in its leaky cache design. In addition, Intel was aware of many research papers that proposed various solutions. Instead of acting, Intel did nothing.

210. As previously discussed, cache side-channel attacks, such as Meltdown, Foreshadow, and Spectre, require fine-grain time measurements to time cache accesses to leak information. Intel includes in the x86 Instruction Set a Read Time-Stamp Counter instruction, or RDTSC which provides high resolution CPU timing information. RDTSC is the instruction used to collect timing information in virtually all cache side-channel attacks.

211. In the '294 patent, Intel recognized the role that RDTSC played in cache side-channel attacks. In particular, Intel acknowledged that "[d]isabling counters almost guarantees that timing-based attacks cannot be executed by Ring 3 [user privilege level] spies." *Id.* at col. 3, l. 14-15. Intel then proposed limiting access to the RDTSC instruction based on privilege "leaving it to the OS [operating system] to determine which applications have the privilege to read timestamp and performance counters." *Id.* at col. 4, l. 19-20.

212. Further, in 2012, Intel was presented with a solution that further restricted access to the fine-grain timekeeping needed to carry out timing side-channel attacks. In Martin, *et al.*, *Timewarp: Rethinking Timekeeping and Performance Monitoring Mechanisms to Mitigate Side-*

Channel Attacks (2012), the authors provide a comprehensive solution that would "limit the fidelity of fine grain timekeeping and performance counters, making it difficult for an attacker to distinguish between different microarchitectural events, thus thwarting attacks." *Id.* at Abstract.

213. The authors noted that, the timing side-channel mitigations "require minor—or in some cases, no—hardware modifications and do not result in any substantial performance degradation, yet offer the most comprehensive protection against microarchitectural side channels to date." *Id.* at Abstract.

214. Intel has proposed other protections to prevent cache side-channel attacks. In the '356 patent, Intel described a scenario that again foreshadows the attacks at issue here and noted that to thwart such an attack, one could prevent repeated evictions from the cache of the victim's data, which is a critical step used in cache side-channel attacks.[65] Intel went on to propose a protected cache design in which a cache controller handles access to, and eviction of, given cache line data based on protection data stored in the cache that controls access to the corresponding cache line.

215. Similarly, in the '201 patent, Intel proposed a protected cache design that acts like "a big private scratchpad intended for the use of the processor to generate intermediate results," in which private data can be tagged as such to prevent it from being chosen as a victim for eviction by an attacker. *Id.* at col.2, l.20-33. Likewise, in the '425 patent, Intel proposed an instruction to

[65] In the described attack, two threads use the same cache such that "when the attacker program is swapped into the processor state in place of the victim program, the data of the victim program in the cache is evicted and vice-versa. [W]hen the attacker program is being swapped in again, it can identify which parts of its own data was evicted by observing the latency of its read operations. By repeating that process, the attacker can infer information about the access patterns of the victim and expose a private key associated with the victim program, thus enabling the attacker program to access the private data of the victim." '356 patent at col.2, l.9-19.

enable applications to monitor sensitive memory locations in cache, and if a monitored location is evicted, the application could then take steps to obscure its access patterns to cache.

216. Another mitigation that Intel was aware of from at least 2010[66] are the cache designs presented by Dr. Lee in Lee, *et al.*, *New cache Designs for Thwarting Software Cache-based Side Channel Attacks* (2007). Lee proposed a cache design that "can defend against cache-based side channel attacks . . . with very little performance degradation and hardware cost." Lee's cache design incorporates a cache partition mechanism, called PLcache, that creates "a flexible 'private partition'" so that "cache lines can not be evicted by other cache accesses not belonging to this private partition." *Id.* at 4.1. Lee also a described a cache design, called RPcache, which employs dynamic random mapping to deny an attacker information about where potential victim code exists in the cache. *Id.* at 4.2. [67]

217. The cache designs proposed by Intel in the '201 Patent, the '356 Patent, and the '425 Patent, as well as the cache designs proposed by Lee, each propose solutions to prevent a spy process from gaining information about a victim process based on data that is evicted from cache. Accordingly, these patents would mitigate the Flush + Reload and Evict + Reload attack techniques used in cache side-channel attacks.

[66] Intel participated in the Hot Chips 26 conference where Dr. Lee presented her cache design. *See* https://www.hotchips.org/archives/2010s/hc26/ (last visited Aug. 24, 2018).

[67] Dr. Lee has received a patent, *Cache Memory Having Enhanced Performance And Security Features*, U.S. 8,549,208, issued Oct. 1, 2013 and published Jul 15, 2010 that describes her secure cache design. Dr. Lee also filed a patent application, *Systems and Methods for Random Fill Caching and Prefetching for Secure Cache Memories*, Pub. No. U.S. 2016/0170889 A1 (filed Dec. 14, 2015), that proposes additional security enhancements.

218. In sum, Intel was fully aware that its leaky cache design posed a substantial security risk from increasingly effective side-channel attacks. It was likewise aware of techniques that could mitigate or thwart variants of such attacks. Yet, it failed to do so.

219. It was only after Meltdown and Spectre became public, and Intel had a "gun to its head," that Intel acquiesced to prospectively change its hardware design to deal with vulnerabilities inherent to its cache design.

D. Intel's Interim Patches Have Impacted the Performance of the CPUs and Still Leave the CPUs Vulnerable to Attack

220. While Intel would like to minimize the scope and severity of the Defects, Plaintiffs and similarly-situated consumers have been harmed, injured, and damaged by Intel's inherently and materially defective CPUs, which allow attackers to steal sensitive data, including passwords and banking information. What makes the security Defects so harmful to Plaintiffs and proving difficult for Intel to mitigate is that—after years of Intel making design and development decisions that placed speed and performance ahead of security (as described above)—the Defects are fully integrated into the design of Intel's CPUs. Thus, because of Intel's actions (and inactions) to address the Defects and safeguard the cache, it is not possible to eliminate the security vulnerabilities and maintain promised performance and high processor clock speeds.

221. Despite its knowledge of the defective CPUs for months, Defendant has been unable or unwilling to repair the Defects without substantial performance degradation or offer Plaintiffs and Class members a non-defective Intel CPU or reimbursement for the cost of such defective CPUs and the consequential damages arising from the purchase and use of the CPUs.

222. Initial fixes were rushed out, with many unintended consequences. Operating system (OS) patches were released, but these caused unacceptable data corruption and loss, and were quickly withdrawn. CPU microcode updates were released, but ended up often disabling

servers – so most customers steered clear of these risky updates. Intel meanwhile promised future CPUs without these flaws would be "available soon"—which of course did nothing to address the millions and millions of vulnerable devices already in the field.

223. Worse still, the patches available dramatically reduce performance of the CPUs. And while the patches dramatically degrade the CPUs' performance, they do not fix the Defects. The existing mitigations leave the door wide open for further exploits which take advantage of the same core Defects involving Intel's processor-caching and memory usage. The patches address only one aspect of the side-channel attacks, leaving available other possible variations to be exploited by attackers. This is why more variants of cache side-channel attacks are still being reported. Since the Meltdown and Spectre attacks were publicly disclosed, numerous new variants of Meltdown, Foreshadow, and Spectre have been announced, including the following:

Class of Attack	**CVE**	**Exploit Name**	**Public Attack Name**
Spectre	2017-5753	Variant 1	Bounds Check Bypass (BCB)
Spectre	2017-5715	Variant 2	Branch Target Injection (BTI)
Meltdown	2017-5754	Variant 3	Rogue Data Cache Load (RDCL)
Spectre-NG	2018-3640	Variant 3a	Rogue System Register Read (RSRE)
Spectre-NG	2018-3639	Variant 4	Speculative Store Bypass (SSB)
Spectre-NG	2018-3665		Lazy FP State Restore

Class of Attack	**CVE**	**Exploit Name**	**Public Attack Name**
Spectre-NG	2018-3693	Variant 1.1	Bounds Check Bypass Store (BCBS)
Spectre		Variant 1.2	Read-only protection bypass (RPB)
SpectreRSB			Return Mispredict
Foreshadow	2018-3615	Variant 5	L1 Terminal Fault-SGX
Foreshadow-NG	2018-3620		L1 Terminal Fault-OS/ SMM
Foreshadow-NG	2018-3646		L1 Terminal Fault-VMM

224. The only true fix is a newly-designed CPU microarchitecture that safeguards processor-caching and memory usage from side-channel attack like many of Intel's competitors' CPUs do. Plaintiffs and Class members are thus left with the unappealing choice of either purchasing a new computer containing a CPU that does not contain the Defects, or continuing to use a computer with massive security vulnerabilities or one with significant performance degradation (by as much as 30 percent).

E. Intel's Failed Mitigation Attempts Have Resulted in Significant Negative Consequences

225. Even after Intel learned of Meltdown and Spectre, it unreasonably delayed disclosing the vulnerability for months, thereby increasing the exposure, risks, and injury to Plaintiffs and Class members. Yet even with such substantial lead-time, Intel was very slow to

provide patches. The mitigations came nearly two months after the CPU vulnerabilities were first exposed publicly and nearly nine months after they were first reported to Intel.

226. Then, when Intel finally did deploy patches months too late, Intel's patches caused systems to reboot unexpectedly and led to data loss and corruption. Intel even advised consumers not to download its patches until better versions were deployed. Intel EVP Neil Shenoy stated that "[w]e recommend that OEMs, cloud service providers, system manufacturers, software vendors, and end users stop deployment of current versions on specific platforms as they may introduce higher than expected reboots and other unpredictable system behavior."[68] Intel then buried a warning in its latest financial results that its buggy firmware updates could lead to "data loss or corruption."[69]

227. Microsoft was also forced to issue out-of-band security updates to deal with the issues around Intel's Spectre firmware updates. Microsoft's Meltdown patches created an even bigger problem in Windows 7 that allowed any unprivileged application to read kernel memory. According to security researcher Ulf Frisk, the faulty patches wrongly set a bit in the virtual-to-physical-memory translator known as PLM4 to allow any user-mode application to access the kernel's page tables.[70]

228. And while it attempted to patch the vulnerabilities caused by its Defects in certain CPUs, Intel chose to wholly ignore numerous systems affected by the Meltdown and the Spectre

[68] https://www.techradar.com/news/dont-download-intels-latest-spectre-and-meltdown-patch-intel-warns (last visited Aug. 24, 2018).

[69] https://www.theverge.com/2018/1/29/16944326/microsoft-spectre-processor-bug-emergency-windows-update-reboot-fix (last visited Aug. 24, 2018).

[70] https://www.zdnet.com/article/windows-7-meltdown-patch-opens-worse-vulnerability-install-march-updates-now/ (last visited Aug. 24, 2018).

class of attacks and leave them vulnerable to exploit. CPU families that Intel will not patch include Bloomfield, Clarksfield, Gulftown, Harpertown Xeon C0, Harpertown Xeon E0, Jasper Forest, Penryn/QC, SoFIA 3GR, Wolfdale C0 and M0, Wolfdale E0 and R0, Wolfdale Xeon X0, Wolfdale Xeon E0, Yorkfield, and Yorkfield Xeon.[71]

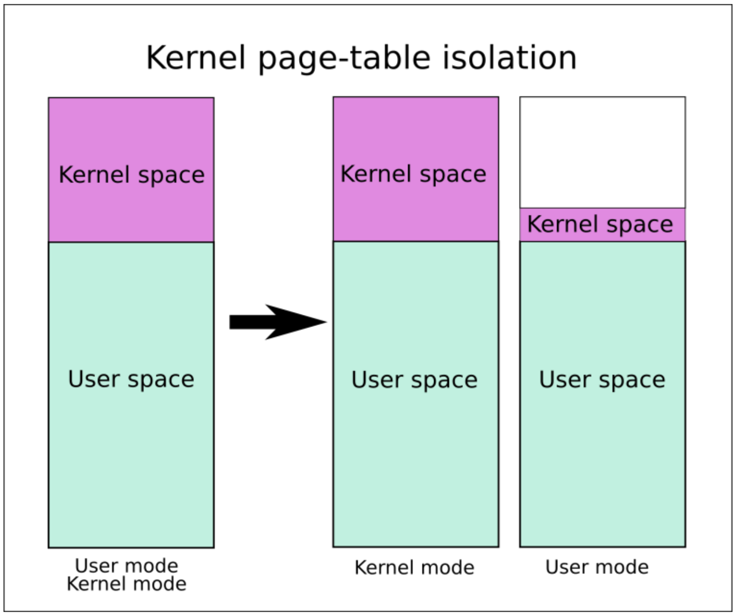
F. Intel's Interim Patches Come at a Significant Cost to the CPUs' Processing Speed and Performance

229. The cache side-channel attacks, including the Meltdown, Foreshadow, and Spectre class of attacks, which exploit the Defects in Intel's CPUs, are not just extraordinary issues of security, but also performance. Intel's mitigations cause substantial performance degradation with some researchers claiming up to 30% loss in performance.

230. The fixes carry performance costs, in part, because the cache side-channel attacks exploit Intel's implementation of speculative execution, which as described above is a physical feature built into the CPUs to speed up operations. Thus, safeguarding against attacks depletes the speed and performance on which Intel distinguished its CPUs.

231. For example, to mitigate the Meltdown attack, Intel recommends changes to operating system kernel code, including increased isolation of kernel memory from user-mode processes. This mitigation is often referred to as kernel page-table isolation ("KPTI," which is also referred to as KAISER). The protection is based on complete separation of kernel and user page tables. As a result, kernel and user programs exist in separate address spaces, effectively mitigating Meltdown, but not the other cache side-channel attacks. KPTI effectively mitigates Meltdown because user applications no longer can perform speculative memory accesses to kernel address space since the kernel is completely unmapped, as depicted below:

[71] https://www.zdnet.com/article/intel-we-now-wont-ever-patch-spectre-variant-2-flaw-in-these-chips/ (last visited Aug. 24, 2018).



232. KPTI protection comes with a substantial performance cost. The performance impact (often referred to as "overhead") of the KPTI patches alone was measured by Dave Hansen, a Linux kernel developer who works at Intel, to be between 5–30%, even with the PCID optimization;[72] for database engine PostgreSQL the impact on read-only tests on an Intel Skylake processor was 7–17% (or 16–23% without PCID),[73] while a full benchmark lost 13–19% (Coffee Lake vs. Broadwell-E).[74]

233. KPTI patches, however, do not protect from any variation of the Foreshadow and Spectre attacks or when Meltdown is performed within the same address space, for example in case of software modules protected with software fault isolation techniques.

[72] https://lwn.net/Articles/738997/ (last visited Aug. 24, 2018).

[73] https://www.postgresql.org/message-id/20180102222354.qikjmf7dvnjgbkxe%40alap3.anarazel.de (last visited Aug. 24, 2018).

[74] https://www.phoronix.com/scan.php?page=article&item=linux-415-x86pti&num=2 (last visited Aug. 24, 2018).

234. To mitigate the Foreshadow attacks, Intel recommends implementing microcode and operating system updates and hypervisor changes (for cloud guests). Foreshadow mitigations enable a new feature called the ESXi Side-Channel-Aware Scheduler, also referred to as the ESXi SCA Scheduler. This scheduler will schedule the hypervisor and VMs on only one logical processor of an Intel Hyper-Threading-enabled core. This means the ESXi Side-Channel-Aware Scheduler will not make use of all the Hyper-Threading cores presented.

235. Like the KPTI patches, the Foreshadow mitigation techniques will impose significant performance overhead. For example, the performance impact observed in test environments for enterprise class workloads after implementing Foreshadow patches and enabling the ESXi Side-Channel-Aware Scheduler was as high as 32%:[75]

Application Workload / Guest OS	**Performance degradation after enabling Foreshadow mitigations**
Database OLTP / Windows	32%
Database OLTP / Linux (with vSAN)	32%
Mixed Workload / Linux	25%
Java / Linux	22%
VDI / Windows	30%

236. Incredibly, aware that the performance impacts of mitigating this severe vulnerability created by its own flawed microarchitecture design decisions would be substantial for many consumers, Intel attempted to impose a licensing restriction to prevent owners of its CPUs from using benchmark software to assess the extent of the performance overhead associated with patching their CPUs to prevent a Foreshadow attack.[76]

[75] https://kb.vmware.com/s/article/55767#q=performance (last visited Aug. 24, 2018).

[76] https://software.intel.com/en-us/protected-download/739797/493768 (last visited Aug. 24, 2018).

237. To mitigate the Spectre attacks, Intel also recommends implementing separate microcode updates and retpoline compiler changes.

238. In total, there are at least four layers of performance overhead related to Intel's mitigations for the Meltdown, Foreshadow, and Spectre attacks. They include:

- Guest kernel KPTI patches
- Intel microcode updates
- Cloud provider hypervisor changes (for cloud guests)
- Retpoline compiler changes

239. Intel's mitigations affect real-world application benchmarks and cause a massive drain on CPU performance.[77] Exactly how much the system is impacted depends on the characteristics of the application being tested. As Brendan Gregg, a senior performance architect at Netflix, explained, applications with higher system call (or syscall) rates, such as proxies and databases that do lots of I/O (input/output), will suffer the largest losses. The impact also rises with higher context switch and page fault rates.[78] For Foreshadow mitigations, the severity of the impact will also depend on the CPU overcommit ratio on a given host and the host utilization.[79]

240. Based on side-by-side comparisons between systems built from different generations of Intel CPUs, the performance overhead caused by Intel's mitigations can take performance back several generations of CPUs.

[77] http://www.brendangregg.com/blog/2018-02-09/kpti-kaiser-meltdown-performance.html (last visited Aug. 24, 2018).

[78] http://www.brendangregg.com/blog/2018-02-09/kpti-kaiser-meltdown-performance.html (last visited Aug. 24, 2018).

[79] https://kb.vmware.com/s/article/55767#q=performance (last visited Aug. 24, 2018).

G. The Only True "Fix" for the Security Vulnerabilities Inherent in Intel's Defective CPUs Is a New CPU

241. Researchers have confirmed that the Meltdown and Foreshadow vulnerabilities are exclusive to Intel CPUs, and that proper implementation of speculative execution would have prevented these attacks.

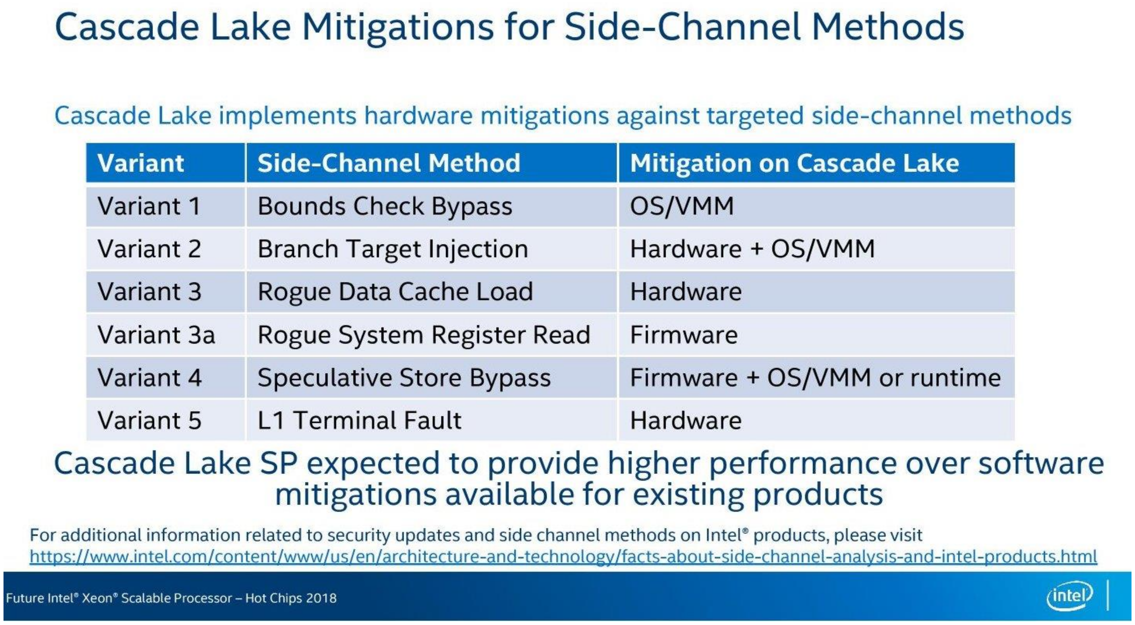
242. Intel's mitigations to date address only one aspect of the cache side-channel attack, leaving attackers with other possible variations that are still available. And while Intel has deployed patches to mitigate Meltdown, Foreshadow, and Spectre attacks, the real fix, according to Intel, is remedying its defective CPU design.[80]

243. Thus, Intel's only *true* fix is a CPU microarchitecture that safeguards processor-caching and memory usage from side-channel attack. To this end, Intel's former CEO Brian Krzanich announced that Intel expects to ship a CPU with hardware fixes for its defective design by the end of 2018. Under Intel's Xeon Roadmap, it plans to release Cascade Lake in 2018, Cooper Lake in 2019, and Ice Lake in 2020.[81]

244. Intel's Cascade Lake will include fixes for Meltdown, Foreshadow, and Spectre and every new CPU features security updates, as follows:

[80] https://kb.vmware.com/s/article/55767#q=performance (last visited Aug. 24, 2018).

[81] https://www.anandtech.com/show/13239/intel-at-hot-chips-2018-showing-the-ankle-of-cascade-lake (last visited Aug. 24, 2018).



Cascade Lake Mitigations for Side-Channel Methods

Cascade Lake implements hardware mitigations against targeted side-channel methods

Variant	Side-Channel Method	Mitigation on Cascade Lake
Variant 1	Bounds Check Bypass	OS/VMM
Variant 2	Branch Target Injection	Hardware + OS/VMM
Variant 3	Rogue Data Cache Load	Hardware
Variant 3a	Rogue System Register Read	Firmware
Variant 4	Speculative Store Bypass	Firmware + OS/VMM or runtime
Variant 5	L1 Terminal Fault	Hardware

Cascade Lake SP expected to provide higher performance over software mitigations available for existing products

For additional information related to security updates and side channel methods on Intel® products, please visit https://www.intel.com/content/www/us/en/architecture-and-technology/facts-about-side-channel-analysis-and-intel-products.html

Future Intel® Xeon® Scalable Processor – Hot Chips 2018

CLASS ACTION ALLEGATIONS

245. Pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), as applicable, and (c)(4), Plaintiffs seek certification of a class initially defined as follows:

> All persons or entities that purchased or leased one or more Intel CPUs or one or more devices containing an Intel CPU in the United States and its territories since January 1, 2006 to the present.

246. If necessary or alternatively, Plaintiffs also seek to represent subclasses of individuals who purchased the Intel CPUs or devices contained the CPUs in each of the 50 states and U.S. territories with representative Plaintiffs as addressed in this Complaint. As detailed below in their respective causes of action, each state subclass is referenced by the name of its state (*i.e.*, the Alabama Subclass, the Washington Subclass, etc.).

247. Collectively, unless otherwise so stated, the above-defined classes and subclasses are referred to herein as the "Class."

248. Excluded from the Class are: (1) Intel, its subsidiaries, affiliates, officers, directors, employees, agents, and contractors; (2) persons or entities that have settled with and validly-

released Intel from separate, non-class legal actions against Intel based on the conduct alleged herein; and (3) the Court and its employees and relatives.

249. Plaintiffs reserve their right to amend the Class definitions if discovery and further investigation reveal that any Class should be expanded or narrowed, divided into additional subclasses under Rule 23(c)(5), or modified in any other way.

250. **Numerosity: Federal Rule of Civil Procedure 23(a)(1).** Class members are so numerous and geographically dispersed that individual joinder of all Class members is impracticable. Plaintiffs are informed and believe—based upon the publicly-available information discussed herein—that there are millions of Class members throughout the country, making joinder impracticable.

251. **Commonality and Predominance: Federal Rules of Civil Procedure 23(a)(2) and 23(b)(3).** Intel has acted with respect to Plaintiffs and the other members of the proposed Class in a manner generally applicable to each of them. There are numerous questions of law and fact common to Plaintiffs and Class members that predominate over any question affecting only individual Class members. The answers to these common questions will advance the adjudication or resolution of the litigation as to all Class members. The questions of law and fact common to the Class that predominate over the questions that may affect individual Class members include the following:

a. Whether Intel engaged in the conduct alleged herein;

b. Whether Intel designed, manufactured, advertised, promoted, and sold CPUs that it knew were defective, and withheld material information regarding the defective nature from consumers or purposefully misrepresented the CPUs to consumers;

c. Whether Intel designed or manufactured the chips in such a way that made them susceptible to security exploits, allowing for side-channel attacks;

d. Whether and to what extent Intel disclosed the effect of the Defects to device security and, ultimately, performance;

e. Whether Intel designed and manufactured CPUs with the Defects that, in turn, created security vulnerabilities as described herein, and whether Intel profited from its shortcuts by inducing Plaintiffs and the other Class members to purchase CPUs that were advertised as secure yet fast;

f. Whether Plaintiffs and absent Class members received the benefit of their bargain in purchasing the Intel CPUs;

g. Whether Intel was under a duty to disclose the true nature of the Intel CPUs to consumers;

h. Whether Intel fraudulently concealed material facts from Plaintiffs and absent Class members;

i. Whether the true nature of the Intel CPUs constitute material facts that reasonable consumers would have considered in deciding whether to purchase the Intel CPUs or computers containing them;

j. Whether Intel's conduct violated consumer protection statutes, false advertising laws, warranty laws, and other common laws asserted herein;

k. Whether Plaintiffs and absent Class members are entitled to equitable relief, including, but not limited to, restitution, declaratory and injunctive relief.

l. Whether Intel has been unjustly enriched as a result of its improper conduct, such that it would be inequitable for Intel to retain the benefits conferred upon it by Plaintiffs and the other Class members;

m. The aggregate compensatory or consequential damages that should be awarded to Plaintiffs and absent Class members; and

n. Whether Intel's conduct in actively suppressing knowledge of the Defects rises to a level of egregiousness that warrants an award of punitive damages.

252. **Typicality: Federal Rule of Civil Procedure 23(a)(3).** Plaintiffs' claims are typical of absent Class members' claims because Plaintiffs and Class members were subjected to the same allegedly unlawful conduct and damaged in the same way. Plaintiffs' claims are based on the same legal theories as the claims of all other members of each of their respective class. Moreover, Plaintiffs seek the same forms of relief for themselves as they do on behalf of absent Class members.

253. **Adequacy of Representation: Federal Rule of Civil Procedure 23(a)(4).** Plaintiffs are adequate class representatives because they assert claims that are typical of those of absent Class members, giving them every incentive to vigorously pursue those claims and protect absent members' interests. Plaintiffs' interests do not conflict with the interests of the other Class members who they seek to represent, the Court has appointed competent counsel pursuant to Rule 23(g) to lead the litigation, and Plaintiffs intend to prosecute this action vigorously. The Class members' interests will be fairly and adequately protected by Plaintiffs and their counsel.

254. **Declaratory and Injunctive Relief: Federal Rule of Civil Procedure 23(b)(2).** The prosecution of separate actions by individual Class members would create a risk of inconsistent or varying adjudications with respect to individual Class members that would

establish incompatible standards of conduct for Intel. Such individual actions would create a risk of adjudications that would be dispositive of the interests of other Class members and impair their interests. Intel has acted and/or refused to act on grounds generally applicable to the Class, making final injunctive relief or corresponding declaratory relief appropriate.

255. Injunctive relief is particularly necessary in this case because: (1) Plaintiffs and absent Class members desire to purchase products with the same qualities and attributes as Intel advertised the Intel CPUs to have; (2) if Intel actually manufactured Intel CPUs with the performance and security advertised, Plaintiffs would purchase those Intel CPUs; (3) Plaintiffs do not, however, have the ability to determine whether Intel's representations concerning the Intel CPUs will be truthful if they purchase Intel CPUs or computers containing Intel CPUs in the future. Indeed, Plaintiffs, and absent Class members may in the future want to purchase Intel CPUs or computers containing Intel CPUs, but they expect that Intel will continue to misrepresent or conceal defects in those processors.

256. **Superiority: Federal Rule of Civil Procedure 23(b)(3).** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiffs and Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Intel, so it would be impracticable for Class members to individually seek redress for Intel's wrongful conduct. Even if Class members could afford to pursue individual litigation, the court system could not handle a deluge of individual suits. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties

and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. The benefits of proceeding on a class-wide basis, including providing injured persons or entities with a method for obtaining redress for claims that might not be practicable to pursue on an individual basis substantially outweigh any potential difficulties in managing this litigation on a class basis.

TOLLING OF APPLICABLE LIMITATIONS PERIODS

257. **Discovery Rule Tolling.** Neither Plaintiffs nor absent Class members could have discovered, through the exercise of reasonable diligence, that their Intel CPUs had serious security Defects within the time period of any applicable statutes of limitation. As described herein, substantial technological expertise is required to uncover the existence of the Defects alleged herein, and the ordinary reasonable consumer could not—with reasonable diligence—discover that their CPUs had systemic Defects and were vulnerable to side-channel attacks until experts started publicly voicing their research and concerns.

258. **Fraudulent Concealment Tolling.** Throughout the time period relevant to this action, Intel concealed from and failed to disclose to Plaintiffs and absent Class members vital information concerning the Intel CPUs. Indeed, Intel kept Plaintiffs and absent Class members ignorant of vital information essential to the pursuit of their claims. As a result, neither Plaintiffs nor absent Class members could have discovered the Defects and security flaws, even upon reasonable exercise of diligence.

259. Despite its knowledge of the above, Intel failed to disclose and concealed, and continues to conceal, critical information from Plaintiffs and absent Class members, even though, at any point in time, it could have communicated material information through individual correspondence, media releases, or other means. Although Intel has finally acknowledged the

security flaw in its chips, it waited years to do so, and has continued to conceal the true risks in using its CPUs.

260. Plaintiffs and absent Class members relied on Intel to disclose any defects in their CPUs, because those defects were hidden and not discoverable through reasonable efforts by Plaintiffs and absent Class members.

261. Thus, the running of all applicable statutes of limitation have been suspended with respect to any claims that Plaintiffs and absent Class members have sustained as a result of the Defects, by virtue of the fraudulent concealment doctrine.

262. **Estoppel.** Intel was under a continuous duty to disclose to Plaintiffs and the other Class members the true nature, quality, and character of its CPUs. Intel, however, concealed the true nature, quality, and character of the CPUs, as described herein. Based upon the foregoing, Intel is estopped from relying on any statutes of limitations in defense of this action.

CLAIMS ALLEGED

NATIONWIDE COUNT I

BREACH OF IMPLIED WARRANTY

263. The Plaintiffs identified above, individually and on behalf of the Nationwide Class, repeat and re-allege all previously alleged paragraphs, as if fully alleged herein. In the alternative, Plaintiffs bring this claim on behalf of the Subclasses.

264. When Plaintiffs and the putative Class members purchased the Intel CPUs and devices containing the Intel CPUs, the Intel CPUs were supposed to not only conform to the promises or affirmations Intel made, but also be adequately labeled, pass without objection in the trade, and be fit for the ordinary purposes for which microprocessors are used.

265. Intel knew that its CPUs would be purchased by consumers and developed the Intel CPUs for consumers' benefit. Intel knew that its chips would be sold by retailers and incorporated into machines by device manufacturers for the ultimate use by consumers. Accordingly, direct privity is not required to bring this cause of action.

266. The Intel CPUs could not conform to the promises or affirmations Intel made regarding speed of the processors without subjecting Plaintiffs and the putative Class members to substantial security risks.

267. Indeed, for the Intel CPUs to operate without objection in the trade, they would need to ensure the security information of known threats, and not allow for certain security vulnerabilities—including side-channel attacks and the Defects described herein.

268. In order to mitigate the security vulnerabilities described herein, Intel recommended certain patches, described above. However, those patches negatively impact CPU performance, and still do not protect against attacks.

269. Because the Intel CPUs contain security vulnerabilities that, if patched, negatively impact processor performance (so that the processors do not operate as represented), the Intel CPUs are not fit for their ordinary purposes.

270. Further the Intel CPUs are not adequately labeled because the labeling failed to disclose the Defects described herein.

271. Intel has been on notice of these issues and Defects through its own internal research and development process, as well as outside researchers who, as described herein, provided notice to Intel about the Defects well before the filing of this complaint.

272. Intel has had the opportunity to cure the Defects in its processors, but has chosen not to do so. Worse yet, when confronted with the Defects as alleged herein, Intel elected to

continue selling the CPUs despite the Defects described herein. Giving Intel additional opportunity to cure the Defects—which it has already shown it cannot do with patches, alone—would only serve to delay the litigation, and is thus impractical and unnecessary.

273. As a result of Intel's breach of its implied warranty, Plaintiffs and the other Class members received goods with substantially impaired value and/or did not receive the benefit of their bargains. Plaintiffs and the other Class members have been damaged as a result of the diminished value of the Intel CPUs.

274. Plaintiffs and the other Class members are entitled to damages and other legal and equitable relief, including, at their election, the purchase price of the Intel CPUs, overpayment, diminution in value, or loss of benefit of the bargain.

NATIONWIDE COUNT II

FRAUD BY CONCEALMENT AND OMISSION
Common Law Claim

275. The Plaintiffs identified above, individually and on behalf of the Nationwide Class, repeat and re-allege all previously alleged paragraphs, as if fully alleged herein. In the alternative, Plaintiffs bring this claim on behalf of the Subclasses.

276. At all relevant times, Intel was engaged in the business of designing, manufacturing, distributing, and selling the CPUs.

277. Intel, acting through its representatives or agents, delivered CPUs to distributors, computer manufacturers, and various other distribution channels.

278. Intel willfully, falsely, and knowingly omitted various material facts regarding the quality and character of the CPUs.

279. Rather than disclosing material facts to Class members, including but not limited to, that in designing its CPUs, it failed to take measures to protect confidential information from

attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks, Intel concealed material information related to the CPUs, and continued manufacturing and selling those CPUs without making any disclosures.

280. Intel omitted material facts to drive up sales and maintain its market power in light of increasing sales from other market competitors such as AMD, as consumers would not purchase its CPUs, or would pay substantially less for them, had consumers known the truth.

281. Plaintiffs and Class members could not have discovered the above information on their own, because Intel was in the exclusive possession of such information until recently which only became public in January 2018, after Plaintiffs and Class members purchased the CPUs.

282. Although Intel had a duty to ensure the accuracy of the release statements published with respect to each new iteration of CPU, and to ensure accuracy of information regarding the performance of its CPUs, it did not fulfill these duties.

283. Plaintiffs and Class members sustained injury due to the purchase of the CPUs and devices containing those CPUs. Specifically, Plaintiffs and Class members put their confidential information at risk by using the Intel CPUs, and otherwise experience degradation to performance levels of their machines by installing recommended patches to their machines. Plaintiffs and Class members are entitled to recover full or partial refunds for the CPUs, or they are entitled to damages for loss of the benefit of the bargain or the diminished value of their CPUs, amounts to be determined at trial.

284. Intel's acts were done wantonly, maliciously, oppressively, deliberately, with intent to defraud; in reckless disregard of the rights of Plaintiffs and the other Class members; and to enrich themselves. Their misconduct warrants an assessment of punitive damages in an amount sufficient to deter such conduct in the future especially given the threat environment created by

consumers' constant need for connectivity. Punitive damages, if assessed, shall be determined according to proof at trial that Intel's acts were done maliciously, oppressively, deliberately, and with intent to defraud, and in reckless disregard of Plaintiffs' and Class members' rights, and in part to enrich itself at the expense of consumers. Intel's acts were done to gain commercial advantage over competitors, and to drive consumers away from consideration of competitor devices. Intel's conduct warrants an assessment of punitive damages in an amount sufficient to deter such conduct in the future.

NATIONWIDE COUNT III

CONSTRUCTIVE FRAUD
Common Law Claim

285. The Plaintiffs identified above, individually and on behalf of the Nationwide Class, repeat and re-allege all previously alleged paragraphs, as if fully alleged herein. In the alternative, Plaintiffs bring this claim on behalf of the Subclasses.

286. This cause of action is brought in the alternative to Plaintiffs' common law fraud claim.

287. At the time Plaintiffs and Class members purchased their CPUs or machines containing the CPUs, Intel concealed and/or failed to disclose material facts to Class members, including, but not limited to, that in designing its CPUs, it failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks.

288. Intel knew, should have known, or was reckless in not knowing, that its representations and omissions would have misled the ordinary, reasonable consumer as its misrepresentations and omissions were material, and a reasonable consumer would rely upon them in making purchasing decisions.

289. Intel had an obligation not to omit or misrepresent Defects in the CPUs because: (a) it was in the sole possession of such material information; (b) the omitted material facts relate to the functionality of the CPUs; (c) it made partial representations regarding the quality of the CPUs in terms of speed and security; and (d) Plaintiffs and Class members relied upon Intel to make full disclosures based upon the relationship between Plaintiffs and Class members, who relied upon Intel's omissions, and were reasonable in doing so, with the full knowledge of Intel that they did and would have been reasonable in doing so.

290. Plaintiffs and Class members did not know—nor could they have known through reasonable diligence—about the material facts alleged herein.

291. Plaintiffs and Class members would have been reasonable in relying on Intel's misrepresentations (and corresponding omissions) in making their purchasing decisions and downloading patches to their devices.

292. Plaintiffs and Class members had a right to rely upon Intel's representations (and corresponding omissions) as Intel was in the exclusive possession of this information, and consumers could not have otherwise known about material facts omitted.

293. Intel breached its duty to Plaintiffs and the other Class members to make full disclosures of material facts.

294. Plaintiffs and Class members sustained damages as a result of their reliance on Intel's omissions and misrepresentations, and Intel's breach of its duty, thus causing Plaintiffs and Class members to sustain actual losses and damages in a sum to be determined at trial.

NATIONWIDE COUNT IV

VIOLATIONS OF THE CONSUMERS LEGAL REMEDIES ACT, Cal. Civ. Code §§ 1750, *et seq.*

295. The Plaintiffs identified above, individually and on behalf of the Nationwide Class, repeat and re-allege all previously alleged paragraphs, as if fully alleged herein. In the alternative, the California Plaintiff(s) brings this claim on behalf of the California Subclass. Excluded from the Nationwide Class, or in the alternative the California Subclass, are Class members whose purchases were not for personal, family or household use.

296. The Consumers Legal Remedies Act, Cal. Civ. Code §§ 1750, *et seq.* ("CLRA"), is a comprehensive statutory scheme that is to be liberally construed to protect consumers against unfair and deceptive business practices in connection with the conduct of businesses providing goods, property or services to consumers primarily for personal, family, or household use.

297. In accordance with the liberal application and construction of the CLRA, application of the CLRA to all Class members is appropriate, given that Intel's conduct as described herein originated from California, the Intel CPUs were designed in California, and Intel's marketing materials were developed in California.

298. Intel is a "person" as defined by Civil Code §§ 1761(c) and 1770, and has provided "services" as defined by Civil Code §§ 1761(b) and 1770.

299. Plaintiffs and the Class members are "consumers" as defined by Civil Code §§ 1761(d) and 1770, and have engaged in a "transaction" as defined by Civil Code §§ 1761(e) and 1770.

300. Intel's acts and practices were intended to and did result in the sales of products and services to Plaintiffs and the Class members in violation of Civil Code § 1770, including:

a. Representing that goods or services have characteristics that they do not have;

b. Representing that goods or services are of a particular standard, quality, or grade when they were not;

c. Advertising goods or services with intent not to sell them as advertised; and

d. Representing that the subject of a transaction has been supplied in accordance with a previous representation when it has not.

301. Intel's misrepresentations and omissions were material because they were likely to deceive reasonable consumers.

302. Had Intel disclosed to Plaintiffs and Class members material facts, including but not limited to, that in designing its CPUs, Intel failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks, Intel would have been unable to continue selling its defective CPUs and it would have been forced to disclose these material facts regarding its CPUs. Plaintiffs and the Class members acted reasonably in relying on Intel's misrepresentations and omissions, the truth of which they could not have discovered with reasonable diligence.

303. As a direct and proximate result of Intel's violations of California Civil Code § 1770, Plaintiffs and Class members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs or machines containing them, and increased time and expense in installing patches to help resolve some of the CPU security issues (at the expense of speed and at risk of crashing their machines), and otherwise purchasing CPUs that were not defective.

304. Intel has already received notice of the Class members' intent to seek damages in compliance with California Civil Code § 1782(a), and, has failed to cure. Intel also received a

supplemental notice pursuant to California Civil Code § 1782 concerning its wrongful conduct as alleged herein by Plaintiffs and the other Class members. Any further notice would be futile because Intel has yet to offer relief to the Class, despite being on notice of its unfair, deceptive, and fraudulent conduct.

305. Plaintiffs, on behalf of themselves and all Class members, seek an order enjoining the acts and practices alleged unlawful herein and reserve their right to amend the complaint to seek damages pursuant to Section 1782(d).

NATIONWIDE COUNT V

VIOLATIONS OF THE CALIFORNIA UNFAIR COMPETITION LAW,
Cal. Bus. & Prof. Code §§ 17200, *et seq.*

306. The Plaintiffs identified above, individually and on behalf of the Class, repeat and re-allege all previously alleged paragraphs, as if fully alleged herein. In the alternative, the California Plaintiff(s) brings this claim on behalf of the California Subclass.

307. In accordance with the liberal application and construction of the UCL, application of the UCL to all Class members is appropriate, given that Intel's headquarters is in Santa Clara, California, Intel's conduct as described herein originated from California, Intel's marketing campaign was devised in California, and the decisions regarding the design of their CPU's — emanated from California.

308. Intel is a "person" as defined by Cal. Bus. & Prof. Code § 17201.

309. Intel violated Cal. Bus. & Prof. Code §§ 17200, *et seq.* ("UCL") by engaging in unlawful, unfair, and deceptive business acts and practices.

310. Intel has engaged in "unfair" business acts or practices by:

a. Knowingly designing, developing, manufacturing, advertising, and selling CPUs with significant Defects that result in security risks, compromising confidential information, and—if patched—slowing down the CPUs so that consumers did not receive the benefit of their bargain;

b. Marketing and selling Intel CPUs that relied upon speculative execution as a means to achieve higher speeds to compete in the CPU market, while at the same time exposing consumers to side-channel security threats solely to increase profits;

c. Permitting instruction execution in the Intel CPUs without first performing and enforcing the appropriate memory access checks as a means to increase processor speed and, accordingly, putting profits over the safety of consumer data;

d. Failing to take steps to secure the CPU architecture from cache side-channel attacks;

e. Making affirmative public representations about the security of Intel CPUs while, at the same time, not ensuring that safety is a priority in its devices;

f. Making affirmative public representations about the speed of Intel CPUs while knowing that, for those CPUs to offer security for consumer data, they would need to be patched, which would reduce processor speed or leave systems corrupted and still vulnerable; and

g. Concealing and/or failing to disclose material facts, including but not limited to, that in designing its CPUs, it failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks.

311. Intel's practices constitute unfair business practices in violation of the UCL because, among other things, they are immoral, unethical, oppressive, unscrupulous, or substantially injurious to consumers and/or any utility of such practices is outweighed by the harm

caused to consumers. Intel's practices violate the legislative policies of the underlying statutes alleged herein: namely, protecting consumers and preventing persons from being injured. Intel's practices caused substantial injury to Plaintiffs and members of the Class and are not outweighed by any benefits, and Plaintiffs and members of the Class could not have reasonably avoided their injuries.

312. Intel has engaged in "unlawful" business acts or practices by violating multiple state laws, including the CLRA, Cal. Civ. Code §§ 1780, *et seq.*, and California common law, as alleged herein.

313. Intel has engaged in fraudulent acts or practices by concealing and/or failing to disclose material facts to Class members, including that in designing its CPUs, it failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks. Intel's fraudulent acts or practices were likely to deceive reasonable consumers.

314. As a result of Defendant's unfair acts or business practices, Plaintiffs have suffered injury in fact and lost money or property.

315. Plaintiffs and Class members seek all monetary and non-monetary relief allowed by law, including restitution stemming from Intel's unfair, unlawful, and fraudulent business practices; declaratory relief; reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable relief.

NATIONWIDE COUNT VI

VIOLATIONS OF CALIFORNIA'S FALSE ADVERTISING LAW,
Cal. Bus. & Prof. Code §§ 17500, *et seq.*

316. The Plaintiffs identified above, individually and on behalf of the Class, repeat and re-allege all previously alleged paragraphs, as if fully alleged herein. In the alternative, the California Plaintiff(s) brings this claim on behalf of the California Subclass.

317. Intel's acts and practices, as described herein, have deceived and/or are likely to continue to deceive Class members and the public. As described throughout this Complaint, Intel misrepresented the CPUs, concealed the CPUs Defects, concealed the security issues with the CPUs, and also concealed and misrepresented the true nature of the CPUs performance and speed.

318. By its actions, Intel disseminated uniform advertising regarding the CPUs based out of California, and governed by California law. The advertising was, by its very nature, unfair, deceptive, untrue, and misleading within the meaning of Cal. Bus. & Prof. Code §§ 17500, *et seq.* Such advertisements were intended to and likely did deceive the consuming public for the reasons detailed herein.

319. The above-described false, misleading, and deceptive advertising Intel disseminated continues to have a likelihood to deceive in that Intel concealed and/or failed to disclose material facts, including that in designing its CPUs, it failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks.

320. Intel continued to misrepresent to consumers that its CPUs were becoming faster and faster, without explanation of the security shortcuts it took to ensure device performance and speed. Had Intel disclosed those issues, rather than falsely advertising the CPUs' properties, consumers would have not purchased or paid significantly less for the CPUs.

321. In making and disseminating the statements alleged herein, Intel knew, or should have known, its representations, advertisements, and statements were untrue and misleading in violation of California law. Plaintiffs and other Class members based their purchasing decisions on Intel's omitted material facts. The revenues to Intel attributable to products sold in those false and misleading advertisements amount to hundreds of millions of dollars. Plaintiffs and Class members were injured in fact and lost money and property as a result.

322. The misrepresentations and non-disclosures by Intel of the material facts described and detailed herein constitute false and misleading advertising and, therefore, constitute violations of Cal. Bus. & Prof Code §§ 17500, *et seq.*

323. As a result of Defendant's unfair business practices, Plaintiffs have suffered injury in fact and lost money or property.

324. Plaintiffs and Class members seek all monetary and non-monetary relief allowed by law, including restitution stemming from Intel's business practices; declaratory relief; reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable relief.

NATIONWIDE COUNT VII

QUASI CONTRACT OR UNJUST ENRICHMENT,
Common Law Claim

325. The Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Class, repeats and re-alleges all previously alleged paragraphs, as if fully alleged herein. In the alternative, Plaintiff brings this claim on behalf of the Subclasses. This claim is brought in the alternative to any potential or future-pleaded contract-based causes of action.

326. Plaintiff and Class members purchased Intel CPUs and devices containing Intel CPUs, and those CPUs were not as Intel represented them to be, enticing Plaintiff and the Class to purchase the CPUs. If Intel had not concealed and/or failed to disclose material facts to Class members, including that in designing its CPUs, it failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks, Plaintiffs and Class members either would not have bought the CPUs (or devices containing the CPUs), or would have paid less for such products.

327. Accordingly, Intel was unjustly enriched by the purchase price of those CPUs to the detriment of Plaintiffs and Class members.

328. Plaintiff and Class members are entitled to damages in the amount Intel was unjustly enriched, to be determined at trial.

CLAIMS ALLEGED ON BEHALF OF THE SUBCLASSES

ALABAMA SUBCLASS COUNT VIII

ALABAMA DECEPTIVE TRADE PRACTICES ACT,
Ala. Code §§ 8-19-1, *et seq*.

329. The Alabama Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Alabama Subclass, repeats and re-alleges all previously alleged paragraphs, as if fully alleged herein.

330. Intel is a "person" as defined by Ala. Code § 8-19-3(5).

331. Plaintiff and the other Alabama Subclass members are "consumers" as defined by Ala. Code § 8-19-3(2).

332. Intel received notice pursuant to Ala. Code § 8-19-10(e) concerning its wrongful conduct as alleged herein by Plaintiff and Alabama Subclass members. However, sending pre-suit notice pursuant to Ala. Code § 8-19-10(e) would have been an exercise in futility for Plaintiff, as

Intel has already been informed of the allegedly unfair and unlawful conduct as described herein as of the date of the first-filed lawsuit, and has yet to offer Class members a remedy in accordance with similar consumer protection statutes.

333. Intel advertised, offered, or sold goods or services in Alabama, and engaged in trade or commerce directly or indirectly affecting the people of Alabama.

334. Intel engaged in deceptive acts and practices in the conduct of trade or commerce, in violation of the Alabama Deceptive Trade Practices Act, Ala. Code § 8-19-5, including:

a. Knowingly designing, developing, manufacturing, advertising, and selling CPUs with significant Defects that result in security risks, compromising consumer data, and—if patched—slowing down the CPUs so that consumers did not receive the benefit of their bargain;

b. Marketing and selling Intel CPUs that relied upon speculative execution as a means to achieve higher speeds to compete in the CPU market, while at the same time exposing consumers to side-channel security threats solely to increase profits;

c. Permitting instruction execution in the Intel CPUs without first performing and enforcing the appropriate memory access checks as a means to increase processor speed and, accordingly, putting profits over the safety of consumer data;

d. Failing to take steps to secure the CPU architecture from cache side-channel attacks;

e. Making affirmative public representations about the security of Intel CPUs while, at the same time, not ensuring that safety is a priority in its devices;

f. Making affirmative public representations about the speed of Intel CPUs while knowing that, for those CPUs to offer security for consumer data, they would need to be patched, which would reduce processor speed or leave systems corrupted and still vulnerable; and

g. Concealing and/or failing to disclose material facts, including but not limited to, that in designing its CPUs, it failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks.

335. Intel's representations and omissions were material because they were likely to deceive ordinary, reasonable consumers.

336. Intel intended to mislead Plaintiff and Alabama Subclass members and induce them to rely on its misrepresentations and omissions.

337. Had Intel disclosed to Plaintiff and Subclass members material facts, including but not limited to, that in designing its CPUs, it failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks, and was otherwise engaged in deceptive, common business practices, Intel would have been unable to continue in business and it would have been forced to disclose the uniform Defects in its CPUs. Instead, Intel represented that its CPUs were continually improving in speed and performed better than other processors on the market. Plaintiff and the Alabama Subclass members acted reasonably in relying on Intel's misrepresentations and omissions, the truth of which they could not have discovered.

338. Intel acted intentionally, knowingly, and maliciously to violate the Alabama Deceptive Trade Practices Act, and recklessly disregarded Plaintiff and Alabama Subclass members' rights. Intel's knowledge of the CPUs' Defects put it on notice that the CPUs were not as it advertised.

339. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiff and Alabama Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and safety issues.

340. Intel's deceptive acts and practices caused substantial injury to Plaintiff and Alabama Subclass members, which they could not reasonably avoid, and which outweighed any benefits to consumers or to competition.

341. Plaintiff and the Alabama Subclass seek all monetary and non-monetary relief allowed by law, including the greater of (a) actual damages or (b) statutory damages of $100; treble damages; injunctive relief; attorneys' fees, costs, and any other relief that is just and proper.

ALASKA SUBCLASS COUNT IX

ALASKA CONSUMER PROTECTION ACT,
Alaska Stat. §§ 45.50.471, *et seq*.

342. The Alaska Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Alaska Subclass, repeats and re-alleges all previously alleged paragraphs, as if fully alleged herein.

343. Intel advertised, offered, or sold goods or services in Alaska and engaged in trade or commerce directly or indirectly affecting the people of Alaska.

344. Alaska Subclass members are "consumers" as defined by Alaska Stat. § 45.50.561(4).

345. Intel received notice pursuant to Alaska Stat. § 45.50.535 concerning its wrongful conduct as alleged herein by Plaintiff and Alaska Subclass members. However, sending pre-suit notice pursuant to Alaska Stat. § 45.50.535 is an exercise in futility for Plaintiff, as Intel has already

been informed of the allegedly unfair and unlawful conduct as described herein as of the date of the first-filed lawsuit, and has yet to offer Subclass members remedy in accordance with similar consumer protection statutes.

346. Intel engaged in unfair or deceptive acts and practices in the conduct of trade or commerce, in violation Alaska Stat. § 45.50.471, including:

a. Knowingly designing, developing, manufacturing, advertising, and selling CPUs with significant Defects that result in security risks, compromising consumer data, and—if patched—slowing down the CPUs so that consumers did not receive the benefit of their bargain;

b. Marketing and selling Intel CPUs that relied upon speculative execution as a means to achieve higher speeds to compete in the CPU market, while at the same time exposing consumers to side-channel security threats solely to increase profits;

c. Permitting instruction execution in the Intel CPUs without first performing and enforcing the appropriate memory access checks as a means to increase processor speed and, accordingly, putting profits over the safety of consumer data;

d. Failing to take steps to secure the CPU architecture from cache side-channel attacks;

e. Making affirmative public representations about the security of Intel CPUs while, at the same time, not ensuring that safety is a priority in its devices;

f. Making affirmative public representations about the speed of Intel CPUs while knowing that, for those CPUs to offer security for consumer data, they would need to be patched, which would reduce processor speed or leave systems corrupted and still vulnerable; and

g. Concealing and/or failing to disclose material facts, including but not limited to, that in designing its CPUs, it failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks.

347. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

348. Intel intended to mislead Plaintiff and Alaska Subclass members and induce them to rely on its misrepresentations and omissions.

349. Intel acted intentionally, knowingly, and maliciously to violate Alaska's Consumer Protection Act, and recklessly disregarded Plaintiff and Alaska Subclass members' rights. Intel's knowledge of the CPU's security and performance issues put it on notice that the CPUs were not as it advertised.

350. As a direct and proximate result of Intel's unfair and deceptive acts and practices, Plaintiff and Alaska Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain, and increased time and expense in dealing with CPU performance and security issues.

351. Plaintiff and the Alaska Subclass seek all monetary and non-monetary relief allowed by law, including the greater of (a) three times their actual damages or (b) statutory damages in the amount of $500; punitive damages; reasonable attorneys' fees and costs; injunctive relief; and any other relief that is necessary and proper.

ARIZONA SUBCLASS COUNT X

ARIZONA CONSUMER FRAUD ACT,
A.R.S. §§ 44-1521, *et seq.*

352. The Arizona Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Arizona Subclass, repeats and re-alleges all previously alleged paragraphs, as if fully alleged herein.

353. Intel is a "person" as defined by A.R.S. § 44-1521(6).

354. Intel advertised, offered, or sold goods or services in Arizona and engaged in trade or commerce directly or indirectly affecting the people of Arizona.

355. Intel engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts affecting the people of Arizona in connection with the sale and advertisement of "merchandise" (as defined in Arizona Consumer Fraud Act, A.R.S. § 44-1521(5)) in violation of A.R.S. § 44-1522(A).

356. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

357. Intel intended to mislead Plaintiff and Arizona Subclass members and induce them to rely on its misrepresentations and omissions.

358. Had Intel disclosed to Plaintiff and Subclass members material facts, including but not limited to, that in designing its CPUs, it failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks, and was otherwise engaged in deceptive, common business practices, Intel would have been unable to continue in business and it would have been forced to disclose the uniform Defects in its CPUs. Instead, Intel represented that its CPUs were continually improving in speed and performed better than other processors on the market. Plaintiff and the Subclass members

acted reasonably in relying on Intel's misrepresentations and omissions, the truth of which they could not have discovered.

359. Intel acted intentionally, knowingly, and maliciously to violate Arizona's Consumer Fraud Act, and recklessly disregarded Plaintiff and Arizona Subclass members' rights. Intel's knowledge of the CPUs' performance and security issues put it on notice that the CPUs were not as it advertised.

360. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiff and Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and safety issues.

361. Plaintiff and Arizona Subclass members seek all monetary and non-monetary relief allowed by law, including compensatory damages; disgorgement; punitive damages; injunctive relief; and reasonable attorneys' fees and costs.

<u>ARKANSAS SUBCLASS COUNT XI</u>

ARKANSAS DECEPTIVE TRADE PRACTICES ACT,
A.C.A. §§ 4-88-101, *et seq*.

362. The Arkansas Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Arkansas Subclass, repeats and re-alleges all previously alleged paragraphs, as if fully alleged herein.

363. Intel is a "person" as defined by A.C.A. § 4-88-102(5).

364. Intel's products and services are "goods" and "services" as defined by A.C.A. §§ 4-88-102(4) and (7).

365. Intel advertised, offered, or sold goods or services in Arkansas and engaged in trade or commerce directly or indirectly affecting the people of Arkansas.

366. The Arkansas Deceptive Trade Practices Act ("ADTPA"), A.C.A. §§ 4-88-101, *et seq.*, prohibits unfair, deceptive, false, and unconscionable trade practices.

367. Intel engaged in acts of deception and false pretense in connection with the sale and advertisement of services in violation of A.C.A. § 4-88-1-8(1) and concealment, suppression and omission of material facts, with intent that others rely upon the concealment, suppression or omission in violation of A.C.A. § 4-88-1-8(2), and engaged in the following deceptive and unconscionable trade practices defined in A.C.A. § 4-88-107:

a. Knowingly designing, developing, manufacturing, advertising, and selling CPUs with significant Defects that result in security risks, compromising consumer data, and—if patched—slowing down the CPUs so that consumers did not receive the benefit of their bargain;

b. Marketing and selling Intel CPUs that relied upon speculative execution as a means to achieve higher speeds to compete in the CPU market, while at the same time exposing consumers to side-channel security threats solely to increase profits;

c. Permitting instruction execution in the Intel CPUs without first performing and enforcing the appropriate memory access checks as a means to increase processor speed and, accordingly, putting profits over the safety of consumer data;

d. Failing to take steps to secure the CPU architecture from cache side-channel attacks;

e. Making affirmative public representations about the security of Intel CPUs while, at the same time, not ensuring that safety is a priority in its devices;

f. Making affirmative public representations about the speed of Intel CPUs while knowing that, for those CPUs to offer security for consumer data, they would need to be patched, which would reduce processor speed or leave systems corrupted and still vulnerable; and

g. Concealing and/or failing to disclose material facts, including but not limited to, that in designing its CPUs, it failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks.

368. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

369. Intel intended to mislead Plaintiff and Arkansas Subclass members and induce them to rely on its misrepresentations and omissions.

370. Had Intel disclosed to Plaintiff and Subclass members material facts, including but not limited to, that in designing its CPUs, it failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks, and was otherwise engaged in deceptive, common business practices, Intel would have been unable to continue in business and it would have been forced to disclose the uniform Defects in its CPUs. Instead, Intel represented that its CPUs were continually improving in speed and performed better than other processors on the market. Plaintiff and the Subclass members acted reasonably in relying on Intel's misrepresentations and omissions, the truth of which they could not have discovered.

371. Intel acted intentionally, knowingly, and maliciously to violate Arkansas's Deceptive Trade Practices Act, and recklessly disregarded Plaintiff and Arkansas Subclass

members' rights. Intel's knowledge of the CPU's performance and safety issues put it on notice that the CPUs were not as it advertised.

372. As a direct and proximate result of Intel's unconscionable, unfair, and deceptive acts or practices and Plaintiff and Arkansas Subclass members' reliance thereon, Plaintiff and Arkansas Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and safety.

373. Plaintiff and the Arkansas Subclass members seek all monetary and non-monetary relief allowed by law, including actual financial losses; injunctive relief; and reasonable attorneys' fees and costs.

COLORADO SUBCLASS COUNT XII

COLORADO CONSUMER PROTECTION ACT,
Colo. Rev. Stat. §§ 6-1-101, *et seq*.

374. The Colorado Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Colorado Subclass, repeats and re-alleges all previously alleged paragraphs, as if fully alleged herein.

375. Intel is a "person" as defined by Colo. Rev. Stat. § 6-1-102(6).

376. Intel engaged in "sales" as defined by Colo. Rev. Stat. § 6-1-102(10).

377. Plaintiff and Colorado Subclass members, as well as the general public, are actual or potential consumers of the products and services offered by Intel or successors in interest to actual consumers.

378. Intel engaged in deceptive trade practices in the course of its business, in violation of Colo. Rev. Stat. § 6-1-105(1), including:

a. Knowingly designing, developing, manufacturing, advertising, and selling CPUs with significant Defects that result in security risks, compromising consumer data, and—if patched—slowing down the CPUs so that consumers did not receive the benefit of their bargain;

b. Marketing and selling Intel CPUs that relied upon speculative execution as a means to achieve higher speeds to compete in the CPU market, while at the same time exposing consumers to side-channel security threats solely to increase profits;

c. Permitting instruction execution in the Intel CPUs without first performing and enforcing the appropriate memory access checks as a means to increase processor speed and, accordingly, putting profits over the safety of consumer data;

d. Failing to take steps to secure the CPU architecture from cache side-channel attacks;

e. Making affirmative public representations about the security of Intel CPUs while, at the same time, not ensuring that safety is a priority in its devices;

f. Making affirmative public representations about the speed of Intel CPUs while knowing that, for those CPUs to offer security for consumer data, they would need to be patched, which would reduce processor speed or leave systems corrupted and still vulnerable; and

g. Concealing and/or failing to disclose material facts, including but not limited to, that in designing its CPUs, it failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks.

379. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

380. Intel intended to mislead Plaintiff and Colorado Subclass members and induce them to rely on its misrepresentations and omissions.

381. Had Intel disclosed to Plaintiff and Subclass members material facts, including but not limited to, that in designing its CPUs, it failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks, and was otherwise engaged in deceptive, common business practices, Intel would have been unable to continue in business and it would have been forced to disclose the uniform Defects in its CPUs. Instead, Intel represented that its CPUs were continually improving in speed and performed better than other processors on the market. Plaintiff and the Subclass members acted reasonably in relying on Intel's misrepresentations and omissions, the truth of which they could not have discovered.

382. Intel acted intentionally, knowingly, and maliciously to violate Colorado's Consumer Protection Act, and recklessly disregarded Plaintiff and Subclass members' rights. Intel's knowledge of the CPUs' performance and security issues put it on notice that the CPUs were not as it advertised.

383. As a direct and proximate result of Intel's deceptive trade practices, Colorado Subclass members suffered injuries to their legally protected interests.

384. Intel's deceptive trade practices significantly impact the public, because Intel is one of the largest CPU manufacturers in the world, with hundreds of thousands of sales of those devices to Colorado consumers.

385. Plaintiff and Colorado Subclass members seek all monetary and non-monetary relief allowed by law, including the greater of: (a) actual damages, or (b) $500, or (c) three times actual damages (for Intel's bad faith conduct); injunctive relief; and reasonable attorneys' fees and costs.

CONNECTICUT SUBCLASS COUNT XIII

CONNECTICUT TRADE PRACTICES ACT,
C.G.S.A. §§ 42-110g, *et seq*.

386. The Connecticut Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Connecticut Subclass, repeats and re-alleges all previously alleged paragraphs, as if fully alleged herein.

387. Intel is a "person" as defined by C.G.S.A. § 42-110a(3).

388. Intel is engaged in "trade" or "commerce" as those terms are defined by C.G.S.A. § 42-110a(4).

389. At the time of filing this Complaint, Plaintiff has sent notice to the Attorney General and Commissioner of Consumer Protection pursuant to C.G.S.A. § 42-110g(c). Plaintiff will provide a file-stamped copy of the Complaint to the Attorney General and Commissioner of Consumer Protection.

390. Intel advertised, offered, or sold goods or services in Connecticut, and engaged in trade or commerce directly or indirectly affecting the people of Connecticut.

391. Intel engaged in deceptive acts and practices and unfair acts and practices in the conduct of trade or commerce, in violation of the C.G.S.A. § 42-110b, including:

a. Knowingly designing, developing, manufacturing, advertising, and selling CPUs with significant Defects that result in security risks, compromising consumer data, and—if patched—slowing down the CPUs so that consumers did not receive the benefit of their bargain;

b. Marketing and selling Intel CPUs that relied upon speculative execution as a means to achieve higher speeds to compete in the CPU market, while at the same time exposing consumers to side-channel security threats solely to increase profits;

c. Permitting instruction execution in the Intel CPUs without first performing and enforcing the appropriate memory access checks as a means to increase processor speed and, accordingly, putting profits over the safety of consumer data;

d. Failing to take steps to secure the CPU architecture from cache side-channel attacks;

e. Making affirmative public representations about the security of Intel CPUs while, at the same time, not ensuring that safety is a priority in its devices;

f. Making affirmative public representations about the speed of Intel CPUs while knowing that, for those CPUs to offer security for consumer data, they would need to be patched, which would reduce processor speed or leave systems corrupted and still vulnerable; and

g. Concealing and/or failing to disclose material facts, including but not limited to, that in designing its CPUs, it failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks.

392. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

393. Intel intended to mislead Plaintiff and Connecticut Subclass members and induce them to rely on its misrepresentations and omissions.

394. Had Intel disclosed to Plaintiff and Subclass members material facts, including but not limited to, that in designing its CPUs, it failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks, and was otherwise engaged in deceptive, common business practices, Intel would have been unable to continue in business and it would have been forced to disclose the uniform Defects in its CPUs. Instead, Intel represented that its CPUs were continually improving in speed and performed better than other processors on the market. Plaintiff and the Subclass members acted reasonably in relying on Intel's misrepresentations and omissions, the truth of which they could not have discovered.

395. Intel acted intentionally, knowingly, and maliciously to violate the Connecticut Unfair Trade Practices Act, and recklessly disregarded Plaintiff and Connecticut Subclass members' rights. Intel's knowledge of the CPUs' performance and security issues put it on notice that the CPUs were not as it advertised.

396. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiff and Connecticut Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with CPU performance and security issues.

397. Intel's deceptive acts and practices caused substantial, ascertainable injury to Plaintiff and Connecticut Subclass members, which they could not reasonably avoid, and which outweighed any benefits to consumers or to competition.

398. Intel's violations of Connecticut law were done with reckless indifference to the Plaintiff and the Connecticut Subclass or was with an intentional or wanton violation of those rights.

399. Plaintiff requests damages in the amount to be determined at trial, including statutory and common law damages, attorneys' fees, and punitive damages.

DELAWARE SUBCLASS COUNT XIV

DELAWARE CONSUMER FRAUD ACT, 6 Del. Code §§ 2513, *et seq.*

400. The Delaware Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Delaware Subclass, repeats and re-alleges all previously alleged paragraphs, as if fully alleged herein.

401. Intel is a "person" that is involved in the "sale" of "merchandise," as defined by 6 Del. Code § 2511(7), (8), and (6).

402. Intel advertised, offered, or sold goods or services in Delaware and engaged in trade or commerce directly or indirectly affecting the people of Delaware.

403. Intel used and employed deception, fraud, false pretense, false promise, misrepresentation, and the concealment, suppression, and omission of material facts with intent that others rely upon such concealment, suppression and omission, in connection with the sale and advertisement of merchandise, in violation of 6 Del. Code § 2513(a).

404. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

405. Intel acted intentionally, knowingly, and maliciously to violate Delaware's Consumer Fraud Act, and recklessly disregarded Plaintiff and Delaware Subclass members' rights.

Intel's knowledge of the CPUs' performance and security issues put it on notice that the CPUs were not as it advertised.

406. Had Intel disclosed to Plaintiff and Subclass members material facts, including but not limited to, that in designing its CPUs, it failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks, and was otherwise engaged in deceptive, common business practices, Intel would have been unable to continue in business and it would have been forced to disclose the uniform Defects in its CPUs. Instead, Intel represented that its CPUs were continually improving in speed and performed better than other processors on the market. Plaintiff and the Subclass members acted reasonably in relying on Intel's misrepresentations and omissions, the truth of which they could not have discovered.

407. Intel's unlawful trade practices were gross, oppressive, and aggravated, and Intel breached the trust of Plaintiff and the Delaware Subclass members.

408. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiff and Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues.

409. Plaintiff and Delaware Subclass members seek all monetary and non-monetary relief allowed by law, including damages under 6 Del. Code § 2525 for injury resulting from the direct and natural consequences of Intel's unlawful conduct; injunctive relief; and reasonable attorneys' fees and costs.

DISTRICT OF COLUMBIA SUBCLASS COUNT XV

DISTRICT OF COLUMBIA CONSUMER PROTECTION PROCEDURES ACT, D.C. Code §§ 28-3904, *et seq.*

410. The District of Columbia Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the District of Columbia Subclass, repeats and re-alleges all previously alleged paragraphs, as if fully alleged herein.

411. Intel is a "person" as defined by D.C. Code § 28-3901(a)(1).

412. Intel is a "merchant" as defined by D.C. Code § 28-3901(a)(3).

413. Plaintiff and District of Columbia Subclass members are "consumers" who purchased or received goods or services for personal, household, or family purposes, as defined by D.C. Code § 28-3901.

414. Intel advertised, offered, or sold goods or services in District of Columbia and engaged in trade or commerce directly or indirectly affecting the people of District of Columbia.

415. Intel engaged in unfair, unlawful, and deceptive trade practices, misrepresentations, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of goods and services in violation of D.C. Code § 28-3904, including:

a. Knowingly designing, developing, manufacturing, advertising, and selling CPUs with significant Defects that result in security risks, compromising consumer data, and—if patched—slowing down the CPUs so that consumers did not receive the benefit of their bargain;

b. Marketing and selling Intel CPUs that relied upon speculative execution as a means to achieve higher speeds to compete in the CPU market, while at the same time exposing consumers to side-channel security threats solely to increase profits;

c. Permitting instruction execution in the Intel CPUs without first performing and enforcing the appropriate memory access checks as a means to increase processor speed and, accordingly, putting profits over the safety of consumer data;

d. Failing to take steps to secure the CPU architecture from cache side-channel attacks;

e. Making affirmative public representations about the security of Intel CPUs while, at the same time, not ensuring that safety is a priority in its devices;

f. Making affirmative public representations about the speed of Intel CPUs while knowing that, for those CPUs to offer security for consumer data, they would need to be patched, which would reduce processor speed or leave systems corrupted and still vulnerable; and

a. Concealing and/or failing to disclose material facts, including but not limited to, that in designing its CPUs, it failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks.

416. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

417. Intel intended to mislead Plaintiff and District of Columbia Subclass members and induce them to rely on its misrepresentations and omissions.

418. The above unfair and deceptive practices and acts by Intel were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and District of Columbia Subclass members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

419. Intel acted intentionally, knowingly, and maliciously to violate the District of Columbia's Consumer Protection Procedures Act, and recklessly disregarded Plaintiff and District of Columbia Subclass members' rights. Intel's knowledge of the CPUs' performance and security issues put it on notice that the CPUs were not as it advertised.

420. As a direct and proximate result of Intel's unfair, unlawful, and deceptive trade practices, Plaintiff and District of Columbia Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with CPU performance and security issues.

421. Plaintiff and District of Columbia Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, restitution, injunctive relief, punitive damages, attorneys' fees and costs, the greater of treble damages or $1500 per violation, and any other relief that the Court deems proper.

FLORIDA SUBCLASS COUNT XVI

FLORIDA DECEPTIVE AND UNFAIR TRADE PRACTICES ACT,
Fla. Stat. §§ 501.201, *et seq.*

422. The Florida Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Florida Subclass, repeats and re-alleges all previously alleged paragraphs, as if fully alleged herein.

423. Plaintiff and Florida Subclass members are "consumers" as defined by Fla. Stat. § 501.203.

424. Intel advertised, offered, or sold goods or services in Florida and engaged in trade or commerce directly or indirectly affecting the people of Florida.

425. Intel engaged in unconscionable, unfair, and deceptive acts and practices in the conduct of trade and commerce, in violation of Fla. Stat. § 501.204(1).

426. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

427. Had Intel disclosed to Plaintiff and Subclass members material facts, including but not limited to, that in designing its CPUs, it failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks, and was otherwise engaged in deceptive, common business practices, Intel would have been unable to continue in business and it would have been forced to disclose the uniform Defects in its CPUs. Instead, Intel represented that its CPUs were continually improving in speed and performed better than other processors on the market. Plaintiff and the Subclass members acted reasonably in relying on Intel's misrepresentations and omissions, the truth of which they could not have discovered.

428. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiff and Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues.

429. Plaintiff and Florida Subclass members seek all monetary and non-monetary relief allowed by law, including actual or nominal damages under Fla. Stat. § 501.21; declaratory and injunctive relief; reasonable attorneys' fees and costs, under Fla. Stat. § 501.2105(1); and any other relief that is just and proper.

GEORGIA SUBCLASS COUNT XVII

GEORGIA UNIFORM DECEPTIVE TRADE PRACTICES ACT,
O.C.G.A. §§ 10-1-390, *et seq.*

430. The Georgia Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Georgia Subclass, repeats and re-alleges all previously alleged paragraphs, as if fully alleged herein.

431. Intel, Plaintiff, and Georgia Subclass members are "persons" within the meaning of § 10-1-371(5) of the Georgia Uniform Deceptive Trade Practices Act ("Georgia UDTPA").

432. Intel received notice pursuant to O.C.G.A. § 10-1-399 concerning its wrongful conduct as alleged herein by Plaintiff and Georgia Subclass members. However, sending pre-suit notice pursuant to O.C.G.A. § 10-1-399 is an exercise in futility for Plaintiff, as Intel has already been informed of the allegedly unfair and unlawful conduct as described herein as of the date of the first-filed lawsuit, and has yet to offer Class members remedy in accordance with similar consumer protection statutes.

433. Intel engaged in deceptive trade practices in the conduct of its business, in violation of O.C.G.A. § 10-1-372(a), including:

a. Knowingly designing, developing, manufacturing, advertising, and selling CPUs with significant Defects that result in security risks, compromising consumer data, and—if patched—slowing down the CPUs so that consumers did not receive the benefit of their bargain;

b. Marketing and selling Intel CPUs that relied upon speculative execution as a means to achieve higher speeds to compete in the CPU market, while at the same time exposing consumers to side-channel security threats solely to increase profits;

c. Permitting instruction execution in the Intel CPUs without first performing and enforcing the appropriate memory access checks as a means to increase processor speed and, accordingly, putting profits over the safety of consumer data;

d. Failing to take steps to secure the CPU architecture from cache side-channel attacks;

e. Making affirmative public representations about the security of Intel CPUs while, at the same time, not ensuring that safety is a priority in its devices;

f. Making affirmative public representations about the speed of Intel CPUs while knowing that, for those CPUs to offer security for consumer data, they would need to be patched, which would reduce processor speed or leave systems corrupted and still vulnerable; and

g. Concealing and/or failing to disclose material facts, including but not limited to, that in designing its CPUs, it failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks.

434. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

435. Intel intended to mislead Plaintiff and Georgia Subclass members and induce them to rely on its misrepresentations and omissions.

436. In the course of its business, Intel engaged in activities with a tendency or capacity to deceive.

437. Intel acted intentionally, knowingly, and maliciously to violate Georgia's Uniform Deceptive Trade Practices Act, and recklessly disregarded Plaintiff and Georgia Subclass

members' rights. Intel's knowledge of the CPUs' performance and security issues put it on notice that the CPUs were not as it advertised.

438. Had Intel disclosed to Plaintiff and Subclass members material facts, including but not limited to, that in designing its CPUs, it failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks, and was otherwise engaged in deceptive, common business practices, Intel would have been unable to continue in business and it would have been forced to disclose the uniform Defects in its CPUs. Instead, Intel represented that its CPUs were continually improving in speed and performed better than other processors on the market. Plaintiff and the Subclass members acted reasonably in relying on Intel's misrepresentations and omissions, the truth of which they could not have discovered.

439. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiff and Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues.

440. Plaintiff and Georgia Subclass members seek all relief allowed by law, including injunctive relief, and reasonable attorneys' fees and costs, under O.C.G.A. § 10-1-373.

<u>HAWAII SUBCLASS COUNT XIII</u>

HAWAII UNFAIR PRACTICES AND UNFAIR COMPETITION ACT,
Haw. Rev. Stat. §§ 480-1, *et seq.*

441. The Hawaii Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Hawaii Subclass, repeats and re-alleges all previously alleged paragraphs, as if fully alleged herein.

442. Plaintiff and Hawaii Subclass members are "consumers" as defined by Haw. Rev. Stat. § 480-1.

443. Plaintiffs, the Hawaii Subclass members, and Intel are "persons" as defined by Haw. Rev. Stat. § 480-1.

444. Intel advertised, offered, or sold goods or services in Hawaii and engaged in trade or commerce directly or indirectly affecting the people of Hawaii.

445. Intel engaged in unfair or deceptive acts or practices, misrepresentations, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of the goods and services purchased by Hawaii Subclass members in violation of Haw. Rev. Stat. § 480-2(a).

446. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

447. Intel intended to mislead Plaintiff and Hawaii Subclass members and induce them to rely on its misrepresentations and omissions.

448. The foregoing unlawful and deceptive acts and practices were immoral, unethical, oppressive, and unscrupulous.

449. Intel acted intentionally, knowingly, and maliciously to violate Hawaii's Unfair Practices and Unfair Competition Act, and recklessly disregarded Plaintiff and Hawaii Subclass members' rights. Intel's knowledge of the CPUs' performance and security issues put it on notice that the CPUs were not as it advertised.

450. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiff and Hawaii Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the

benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues.

451. Plaintiff and Hawaii Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, benefit of the bargain damages, treble damages, injunctive relief, and reasonable attorneys' fees and costs.

HAWAII SUBCLASS COUNT IXX

HAWAII UNIFORM DECEPTIVE TRADE PRACTICE ACT,
Haw. Rev. Stat. §§ 481A-3, *et seq.*

452. The Hawaii Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Hawaii Subclass, repeats and re-alleges all previously alleged paragraphs, as if fully alleged herein.

453. Plaintiff and Hawaii Subclass members are "persons" as defined by Haw. Rev. Stat. § 481A-2.

454. Intel engaged in unfair and deceptive trade practices in the conduct of its business, violating Haw. Rev. Stat. § 481A-3, including:

a. Knowingly designing, developing, manufacturing, advertising, and selling CPUs with significant Defects that result in security risks, compromising consumer data, and—if patched—slowing down the CPUs so that consumers did not receive the benefit of their bargain;

b. Marketing and selling Intel CPUs that relied upon speculative execution as a means to achieve higher speeds to compete in the CPU market, while at the same time exposing consumers to side-channel security threats solely to increase profits;

c. Permitting instruction execution in the Intel CPUs without first performing and enforcing the appropriate memory access checks as a means to increase processor speed and, accordingly, putting profits over the safety of consumer data;

d. Failing to take steps to secure the CPU architecture from cache side-channel attacks;

e. Making affirmative public representations about the security of Intel CPUs while, at the same time, not ensuring that safety is a priority in its devices;

f. Making affirmative public representations about the speed of Intel CPUs while knowing that, for those CPUs to offer security for consumer data, they would need to be patched, which would reduce processor speed or leave systems corrupted and still vulnerable; and

g. Concealing and/or failing to disclose material facts, including but not limited to, that in designing its CPUs, it failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks.

455. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

456. The above unfair and deceptive practices and acts by Intel were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Hawaii Subclass members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

457. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiff and Subclass members have suffered and will continue to suffer injury, ascertainable losses of money

or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues.

458. Plaintiff and Hawaii Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief, attorneys' fees and costs, and any other relief that the Court deems proper.

IDAHO SUBCLASS COUNT XX

IDAHO CONSUMER PROTECTION ACT,
Idaho Code §§ 48-601, *et seq.*

459. The Idaho Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Idaho Subclass, repeats and re-alleges all previously alleged paragraphs, as if fully alleged herein.

460. Intel is a "person" as defined by Idaho Code § 48-602(1).

461. Intel's conduct as alleged herein pertained to "goods" and "services" as defined by Idaho Code § 48-602(6) and (7).

462. Intel advertised, offered, or sold goods or services in Idaho and engaged in trade or commerce directly or indirectly affecting the people of Idaho.

463. Intel engaged in unfair and deceptive acts or practices, and unconscionable acts and practices, in the conduct of trade and commerce with respect to the sale and advertisement of goods and services, in violation of Idaho Code §§ 48-603 and 48-603(C), including:

a. Knowingly designing, developing, manufacturing, advertising, and selling CPUs with significant Defects that result in security risks, compromising consumer data, and—if patched—slowing down the CPUs so that consumers did not receive the benefit of their bargain;

b. Marketing and selling Intel CPUs that relied upon speculative execution as a means to achieve higher speeds to compete in the CPU market, while at the same time exposing consumers to side-channel security threats solely to increase profits;

c. Permitting instruction execution in the Intel CPUs without first performing and enforcing the appropriate memory access checks as a means to increase processor speed and, accordingly, putting profits over the safety of consumer data;

d. Failing to take steps to secure the CPU architecture from cache side-channel attacks;

e. Making affirmative public representations about the security of Intel CPUs while, at the same time, not ensuring that safety is a priority in its devices;

f. Making affirmative public representations about the speed of Intel CPUs while knowing that, for those CPUs to offer security for consumer data, they would need to be patched, which would reduce processor speed or leave systems corrupted and still vulnerable; and

g. Concealing and/or failing to disclose material facts, including but not limited to, that in designing its CPUs, it failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks.

464. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

465. Intel intended to mislead Plaintiff and Idaho Subclass members and induce them to rely on its misrepresentations and omissions. Intel knew its representations and omissions were false.

466. Intel acted intentionally, knowingly, and maliciously to violate Idaho's Consumer Protection Act, and recklessly disregarded Plaintiff and Idaho Subclass members' rights. Intel's knowledge of the CPUs' performance and security issues put it on notice that the CPUs were not as it advertised.

467. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiff and Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues.

468. Plaintiff and Idaho Subclass members seek all monetary and non-monetary relief allowed by law, including damages, punitive damages, injunctive relief, costs, and attorneys' fees.

ILLINOIS SUBCLASS COUNT XXI

ILLINOIS CONSUMER FRAUD AND DECEPTIVE BUSINESS PRACTICES ACT, 815 ILCS §§ 505, *et seq.*

469. The Illinois Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Illinois Subclass, repeats and re-alleges all previously alleged paragraphs, as if fully alleged herein.

470. Intel is a "person" as defined by 815 ILCS §§ 505/1(c).

471. Plaintiff and Illinois Subclass members are "consumers" as defined by 815 ILCS §§ 505/1(e).

472. Intel's conduct as described herein was in the conduct of "trade" or "commerce" as defined by 815 ILCS § 505/1(f). Intel's conduct is described in full detail above.

473. Intel's deceptive, unfair, and unlawful trade acts or practices, in violation of 815 ILCS § 505/2.

474. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

475. Intel intended to mislead Plaintiff and Illinois Subclass members and induce them to rely on its misrepresentations and omissions.

476. The above unfair and deceptive practices and acts by Intel were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury that these consumers could not reasonably avoid; this substantial injury outweighed any benefit to consumers or to competition.

477. Intel acted intentionally, knowingly, and maliciously to violate Illinois's Consumer Fraud Act, and recklessly disregarded Plaintiff and Illinois Subclass members' rights. Intel's knowledge of the CPUs' performance and security issues put it on notice that the CPUs were not as it advertised.

478. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiff and Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issue.

479. Plaintiff and Illinois Subclass members seek all monetary and non-monetary relief allowed by law, including damages, restitution, punitive damages, injunctive relief, and reasonable attorneys' fees and costs.

ILLINOIS SUBCLASS COUNT XXII

ILLINOIS UNIFORM DECEPTIVE TRADE PRACTICES ACT, 815 ILCS §§ 510/2, *et seq.*

480. The Illinois Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Illinois Subclass, repeats and re-alleges all previously alleged paragraphs, as if fully alleged herein.

481. Intel is a "person" as defined by 815 ILCS §§ 510/1(5).

482. Intel engaged in deceptive trade practices in the conduct of its business, in violation of 815 ILCS §§ 510/2(a), including:

a. Knowingly designing, developing, manufacturing, advertising, and selling CPUs with significant Defects that result in security risks, compromising consumer data, and—if patched—slowing down the CPUs so that consumers did not receive the benefit of their bargain;

b. Marketing and selling Intel CPUs that relied upon speculative execution as a means to achieve higher speeds to compete in the CPU market, while at the same time exposing consumers to side-channel security threats solely to increase profits;

c. Permitting instruction execution in the Intel CPUs without first performing and enforcing the appropriate memory access checks as a means to increase processor speed and, accordingly, putting profits over the safety of consumer data;

d. Failing to take steps to secure the CPU architecture from cache side-channel attacks;

e. Making affirmative public representations about the security of Intel CPUs while, at the same time, not ensuring that safety is a priority in its devices;

f. Making affirmative public representations about the speed of Intel CPUs while knowing that, for those CPUs to offer security for consumer data, they would need to be patched, which would reduce processor speed or leave systems corrupted and still vulnerable; and

g. Concealing and/or failing to disclose material facts, including but not limited to, that in designing its CPUs, it failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks.

483. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

484. The above unfair and deceptive practices and acts by Intel were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Illinois Subclass members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

485. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiff and Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues.

486. Plaintiff and Illinois Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief and reasonable attorney's fees.

INDIANA SUBCLASS COUNT XXIII

INDIANA DECEPTIVE CONSUMER SALES ACT, Ind. Code §§ 24-5-0.5-1, *et seq.*

487. The Indiana Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Indiana Subclass, repeats and re-alleges all previously alleged paragraphs, as if fully alleged herein.

488. Intel is a "person" as defined by Ind. Code § 24-5-0.5-2(a)(2).

489. Intel is a "supplier" as defined by § 24-5-0.5-2(a)(1), because it regularly engages in or solicits "consumer transactions" within the meaning of § 24-5-0.5-2(a)(3)(A).

490. Intel engaged in unfair, abusive, and deceptive acts, omissions, and practices in connection with consumer transactions, in violation of Ind. Code § 24-5-0.5-3(a).

491. Intel's representations and omissions include both implicit and explicit representations and were carried out as a scheme or artifice to defraud.

492. Intel's acts and practices were "unfair" because they caused or were likely to cause substantial injury to consumers which was not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.

493. The injury to consumers from Intel's conduct was and is substantial because it was non-trivial and non-speculative; and involved a monetary injury. The injury to consumers was substantial not only because it inflicted harm on a significant and unprecedented number of consumers, but also because it inflicted a significant amount of harm on each consumer.

494. Consumers could not have reasonably avoided injury because Intel's business acts and practices unreasonably created or took advantage of an obstacle to the free exercise of consumer decision-making. By withholding important information from consumers about the performance and security of its CPUs, and Defects within those processors, Intel created an

asymmetry of information between it and consumers that precluded consumers from taking action to avoid or mitigate injury.

495. Intel’s business practices, in concealing material information or misrepresenting the qualities, characteristics, and performance of its CPUs, had no countervailing benefit to consumers or to competition.

496. Intel’s acts and practices were “abusive” for numerous reasons, including: (a) because they materially interfered with consumers’ ability to understand a term or condition in a consumer transaction, interfering with consumers’ decision-making; (b) because they took unreasonable advantage of consumers’ lack of understanding about the material risks, costs, or conditions of a consumer transaction; consumers lacked an understanding of the material risks and costs of a variety of their transactions; (c) because they took unreasonable advantage of consumers’ inability to protect their own interests; consumers could not protect their interests due to the asymmetry in information between them and Intel; (d) because Intel took unreasonable advantage of consumers’ reasonable reliance that it was providing truthful and accurate information.

497. Intel also engaged in “deceptive” acts and practices in violation of Indiana Code § 24-5-0.5-3(a) and § 24-5-0.5-3(b), including: (a) misrepresenting that the subject of a consumer transaction has sponsorship, approval, performance, characteristics, accessories, uses, or benefits it does not have which the supplier knows or should reasonably know it does not have; (b) misrepresenting that the subject of a consumer transaction is of a particular standard, quality, grade, style, or model, if it is not and if the supplier knows or should reasonably know that it is not; and (c) misrepresenting that the subject of a consumer transaction will be supplied to the public in greater quantity (i.e., greater speed) than the supplier intends or reasonably expects.

498. Intel intended to mislead Plaintiff and Indiana Subclass members and induce them to rely on its misrepresentations and omissions.

499. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

500. Had Intel disclosed to Plaintiff and Subclass members material facts, including but not limited to, that in designing its CPUs, it failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks, and was otherwise engaged in deceptive, common business practices, Intel would have been unable to continue in business and it would have been forced to disclose the uniform Defects in its CPUs. Instead, Intel represented that its CPUs were continually improving in speed and performed better than other processors on the market. Plaintiff and the Subclass members acted reasonably in relying on Intel's misrepresentations and omissions, the truth of which they could not have discovered.

501. Intel had a duty to disclose the above-described facts due to the circumstances of this case, the sensitivity and extensiveness of the Defects in its CPUs, and the generally-accepted standards regarding product safety. Intel's duty to disclose also arose from its: (a) possession of exclusive knowledge regarding the Defects in its CPUs; (b) active concealment of the CPU Defects; (c) incomplete representations about CPU security and performance, while purposefully withholding material facts from Plaintiff and the Indiana Subclass that contradicted these representations.

502. Intel acted intentionally, knowingly, and maliciously to violate Indiana's Deceptive Consumer Sales Act, and recklessly disregarded Plaintiff and Indiana Subclass members' rights.

Intel's knowledge of the CPUs' performance and security issues put it on notice that the CPUs were not as it advertised.

503. Intel received notice pursuant to Ind. Code § 24-5-0.5-5 concerning its wrongful conduct as alleged herein by Plaintiff and Indiana Subclass members. Intel has had constructive notice of Plaintiff's demand for relief for the Indiana Subclass pursuant to Ind. Code § 24-5-0.5-5 since the filing of the first case, which contained substantially similar allegations. Accordingly, sending pre-suit notice pursuant to Ind. Code § 24-5-0.5-5 is an exercise in futility for Plaintiff, as Intel has not cured its unfair, abusive, and deceptive acts and practices, or its violations of Indiana Deceptive Consumer Sales Act were incurable.

504. Intel's conduct includes incurable deceptive acts that Intel engaged in as part of a scheme, artifice, or device with intent to defraud or mislead, under Ind. Code § 24-5-0.5-2(a)(8).

505. As a direct and proximate result of Intel's uncured or incurable unfair, abusive, and deceptive acts or practices, Plaintiff and Indiana Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with CPU performance and security issues.

506. Intel's violations present a continuing risk to Plaintiff and Indiana Subclass members as well as to the general public.

507. Plaintiff and Indiana Subclass members seek all monetary and non-monetary relief allowed by law, including the greater of actual damages or $500 for each non-willful violation; the greater of treble damages or $1,000 for each willful violation; restitution; reasonable attorneys' fees and costs; injunctive relief; and punitive damages.

IOWA SUBCLASS COUNT XXIV

IOWA PRIVATE RIGHT OF ACTION FOR CONSUMER FRAUDS ACT, Iowa Code § 714H

508. The Iowa Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Iowa Subclass, repeats and re-alleges all previously alleged paragraphs, as if fully alleged herein.

509. Intel is a "person" as defined by Iowa Code § 714H.2(7).

510. Plaintiff and Iowa Subclass members are "consumers" as defined by Iowa Code § 714H.2(3).

511. Intel's conduct described herein related to the "sale" or "advertisement" of "merchandise" as defined by Iowa Code §§ 714H.2(2), (6), & (8).

512. Intel engaged in unfair, deceptive, and unconscionable trade practices, in violation of the Iowa Private Right of Action for Consumer Frauds Act, as described throughout and herein.

513. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

514. Intel intended to mislead Plaintiff and Iowa Subclass members and induce them to rely on its misrepresentations and omissions.

515. Intel acted intentionally, knowingly, and maliciously to violate Iowa's Private Right of Action for Consumer Frauds Act, and recklessly disregarded Plaintiff and Iowa Subclass members' rights. Intel's knowledge of the CPU performance and security issues put it on notice that the CPUs were not as it advertised.

516. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiff and Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of

their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues

517. Plaintiff has provided the requisite notice to the Iowa Attorney General, the office of which approved the filing of this class action lawsuit pursuant to Iowa Code § 714H.7.

518. Plaintiff and Iowa Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief, damages, punitive damages, and reasonable attorneys' fees and costs.

KANSAS SUBCLASS COUNT XXV

KANSAS CONSUMER PROTECTION ACT,
K.S.A. §§ 50-623, *et seq.*

519. The Kansas Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Kansas Subclass, repeats and re-alleges all previously alleged paragraphs, as if fully alleged herein.

520. K.S.A. §§ 50-623, *et seq.* is to be liberally construed to protect consumers from suppliers who commit deceptive and unconscionable practices.

521. Plaintiff and Kansas Subclass members are "consumers" as defined by K.S.A. § 50-624(b).

522. The acts and practices described herein are "consumer transactions," as defined by K.S.A. § 50-624(c).

523. Intel is a "supplier" as defined by K.S.A. § 50-624(l).

524. Intel advertised, offered, or sold goods or services in Kansas and engaged in trade or commerce directly or indirectly affecting the people of Kansas.

525. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

526. Intel intended to mislead Plaintiff and Kansas Subclass members and induce them to rely on its misrepresentations and omissions.

527. Had Intel disclosed to Plaintiff and Subclass members material facts, including but not limited to, that in designing its CPUs, it failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks, and was otherwise engaged in deceptive, common business practices, Intel would have been unable to continue in business and it would have been forced to disclose the uniform Defects in its CPUs. Instead, Intel represented that its CPUs were continually improving in speed and performed better than other processors on the market. Plaintiff and the Subclass members acted reasonably in relying on Intel's misrepresentations and omissions, the truth of which they could not have discovered.

528. Intel also engaged in unconscionable acts and practices in connection with a consumer transaction, in violation of K.S.A. § 50-627, including: knowingly taking advantage of the inability of Plaintiff and the Kansas Subclass to reasonably protect their interests, due to their lack of knowledge (*see* K.S.A. § 50-627(b)(1)); and requiring Plaintiff and the Kansas Subclass to enter into a consumer transaction on terms that Intel knew were substantially one-sided in favor of Intel (*see* K.S.A. § 50-627(b)(5)).

529. Plaintiff and the Kansas Subclass had unequal bargaining power with respect to their purchase and/or use of Intel's CPUs because of Intel's omissions and misrepresentations.

530. The above unfair, deceptive, and unconscionable practices and acts by Intel were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Kansas Subclass members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

531. Intel acted intentionally, knowingly, and maliciously to violate Kansas's Consumer Protection Act, and recklessly disregarded Plaintiff and Kansas Subclass members' rights. Intel's knowledge of the CPUs' security and performance issue put it on notice that the CPUs were not as it advertised.

532. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiff and Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues.

533. Plaintiff and Kansas Subclass members seek all monetary and non-monetary relief allowed by law, including civil penalties or actual damages (whichever is greater), under K.S.A. §§ 50-634 and 50-636; injunctive relief; and reasonable attorneys' fees and costs.

<u>KENTUCKY SUBCLASS COUNT XXVI</u>

KENTUCKY CONSUMER PROTECTION ACT,
Ky. Rev. Stat. §§ 367.110, *et seq.*

534. The Kentucky Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Kentucky Subclass, repeats and re-alleges all previously alleged paragraphs, as if fully alleged herein.

535. Intel is a "person" as defined by Ky. Rev. Stat. § 367.110(1).

536. Intel advertised, offered, or sold goods or services in Kentucky and engaged in trade or commerce directly or indirectly affecting the people of Kentucky, as defined by Ky. Rev. Stat. § 367.110(2).

537. Intel engaged in unfair, false, misleading, deceptive, and unconscionable acts or practices, in violation of Ky. Rev. Stat. § 367.170, as described herein.

538. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

539. Intel intended to mislead Plaintiff and Kentucky Subclass members and induce them to rely on its misrepresentations and omissions.

540. Plaintiff and Kentucky Subclass members' purchased goods or services for personal, family, or household purposes and suffered ascertainable losses of money or property as a result of Intel's unlawful acts and practices.

541. The above unlawful acts and practices by Intel were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Kentucky Subclass members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

542. Intel acted intentionally, knowingly, and maliciously to violate Kentucky's Consumer Protection Act, and recklessly disregarded Plaintiff and Kentucky Subclass members' rights. Intel's knowledge of the CPUs' security and performance issues put it on notice that the CPUs were not as it advertised.

543. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiff and Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues.

544. Plaintiff and Kentucky Subclass members seek all monetary and non-monetary relief allowed by law, including damages, punitive damages, restitution or other equitable relief, injunctive relief, and reasonable attorneys' fees and costs.

LOUISIANA SUBCLASS COUNT XXVII

LOUISIANA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION LAW, La. Rev. Stat. Ann. §§ 51:1401, *et seq.*

545. The Louisiana Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Louisiana Subclass, repeats and re-alleges all previously alleged paragraphs, as if fully alleged herein.

546. Intel, Plaintiff, and the Louisiana Subclass members are "persons" within the meaning of the La. Rev. Stat. Ann. § 51:1402(8).

547. Plaintiff and Louisiana Subclass members are "consumers" within the meaning of La. Rev. Stat. Ann. § 51:1402(1).

548. Intel engaged in "trade" or "commerce" within the meaning of La. Rev. Stat. Ann. § 51:1402(10).

549. The Louisiana Unfair Trade Practices and Consumer Protection Law ("Louisiana CPL") makes unlawful "unfair or deceptive acts or practices in the conduct of any trade or commerce." La. Rev. Stat. Ann. § 51:1405(A). Unfair acts are those that offend established public policy, while deceptive acts are practices that amount to fraud, deceit, or misrepresentation.

550. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

551. Intel intended to mislead Plaintiff and Louisiana Subclass members and induce them to rely on its misrepresentations and omissions.

552. Intel's unfair and deceptive acts and practices were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Kentucky Subclass members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

553. Intel acted intentionally, knowingly, and maliciously to violate Unfair Trade Practices and Consumer Protection Law, and recklessly disregarded Plaintiff and Louisiana Subclass members' rights. Intel's knowledge of the CPUs' security and performance issues put it on notice that the CPUs were not as it advertised.

554. Had Intel disclosed to Plaintiff and Subclass members material facts, including but not limited to, that in designing its CPUs, it failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks, and was otherwise engaged in deceptive, common business practices, Intel would have been unable to continue in business and it would have been forced to disclose the uniform Defects in its CPUs. Instead, Intel represented that its CPUs were continually improving in speed and performed better than other processors on the market. Plaintiff and the Subclass members acted reasonably in relying on Intel's misrepresentations and omissions, the truth of which they could not have discovered.

555. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiff and Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues.

556. Plaintiff and Louisiana Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages; treble damages for Intel's knowing violations of the Louisiana CPL; declaratory relief; attorneys' fees; and any other relief that is just and proper.

MAINE SUBCLASS COUNT XXVIII

MAINE UNFAIR TRADE PRACTICES ACT,
5 Me. Rev. Stat. §§ 205, 213, *et seq.*

557. The Maine Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Maine Subclass, repeats and re-alleges all previously alleged paragraphs, as if fully alleged herein.

558. Intel is a "person" as defined by 5 Me. Stat. § 206(2).

559. Intel's conduct as alleged herein related was in the course of "trade and commerce" as defined by 5 Me. Stat. § 206(3).

560. Plaintiff and Maine Subclass members purchased goods and/or services for personal, family, and/or household purposes.

561. A demand for relief in the form substantially similar to that required by 5 Me. Rev. Stat. § 213(1-A) was already sent at the commencement of this lawsuit but Intel has not made a written tender of settlement or offer of judgment. Intel received supplemental notice pursuant to 5 Me. Rev. Stat. § 213(1-A) concerning its wrongful conduct as alleged herein by Plaintiff and Maine Subclass members, but this and any subsequent demand was and would be an exercise in futility.

562. Intel engaged in unfair and deceptive trade acts and practices in the conduct of trade or commerce, in violation of 5 Me. Rev. Stat. §207.

563. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

564. Had Intel disclosed to Plaintiff and Subclass members material facts, including but not limited to, that in designing its CPUs, it failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to

such attacks, and was otherwise engaged in deceptive, common business practices, Intel would have been unable to continue in business and it would have been forced to disclose the uniform Defects in its CPUs. Instead, Intel represented that its CPUs were continually improving in speed and performed better than other processors on the market. Plaintiff and the Subclass members acted reasonably in relying on Intel's misrepresentations and omissions, the truth of which they could not have discovered.

565. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiff and Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues.

566. Plaintiff and the Maine Subclass members seek all monetary and non-monetary relief allowed by law, including damages or restitution, injunctive and other equitable relief, and attorneys' fees and costs.

MAINE SUBCLASS COUNT IXXX

MAINE UNIFORM DECEPTIVE TRADE PRACTICES ACT,
10 Me. Rev. Stat. §§ 1212, *et seq.*

567. The Maine Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Maine Subclass, repeats and re-alleges all previously alleged paragraphs, as if fully alleged herein.

568. Intel is a "person" as defined by 10 Me. Rev. Stat. § 1211(5).

569. Intel advertised, offered, or sold goods or services in Maine and engaged in trade or commerce directly or indirectly affecting the people of Maine.

570. Intel engaged in deceptive trade practices in the conduct of its business, in violation of 10 Me. Rev. Stat. § 1212, including: representing that goods or services have characteristics that they do not have; representing that goods or services are of a particular standard, quality, or grade if they are of another; advertising goods or services with intent not to sell them as advertised; and engaging in other conduct that creates a likelihood of confusion or misunderstanding.

571. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

572. Intel intended to mislead Plaintiff and Maine Subclass members and induce them to rely on its misrepresentations and omissions.

573. Had Intel disclosed to Plaintiff and Subclass members material facts, including but not limited to, that in designing its CPUs, it failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks, and was otherwise engaged in deceptive, common business practices, Intel would have been unable to continue in business and it would have been forced to disclose the uniform Defects in its CPUs. Instead, Intel represented that its CPUs were continually improving in speed and performed better than other processors on the market. Plaintiff and the Subclass members acted reasonably in relying on Intel's misrepresentations and omissions, the truth of which they could not have discovered.

574. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiff and Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues.

575. Maine Subclass members are likely to be damaged by Intel's ongoing deceptive trade practices.

576. Plaintiff and the Maine Subclass members seek all monetary and non-monetary relief allowed by law, including damages or restitution, injunctive or other equitable relief, and attorneys' fees and costs.

MARYLAND SUBCLASS COUNT XXX

MARYLAND CONSUMER PROTECTION ACT,
Md. Comm. Code §§ 13-301, *et seq.*

577. The Maryland Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Maryland Subclass, repeats and re-alleges all previously alleged paragraphs, as if fully alleged herein.

578. Intel is a person as defined by Md. Comm. Code § 13-101(h).

579. Intel's conduct as alleged herein related to "sales," "offers for sale," or "bailment" as defined by Md. Comm. Code § 13-101(i) and § 13-303.

580. Maryland Subclass members are "consumers" as defined by Md. Comm. Code § 13-101(c).

581. Intel advertises, offers, or sell "consumer goods" or "consumer services" as defined by Md. Comm. Code § 13-101(d).

582. Intel advertised, offered, or sold goods or services in Maryland and engaged in trade or commerce directly or indirectly affecting the people of Maryland.

583. Intel engaged in unfair and deceptive trade practices, in violation of Md. Comm. Code § 13-301, including: (a) false or misleading oral or written representations that have the capacity, tendency, or effect of deceiving or misleading consumers; (b) representing that consumer goods or services have a characteristic that they do not have; (c) representing that consumer goods

or services are of a particular standard, quality, or grade that they are not; (d) failing to state a material fact where the failure deceives or tends to deceive; (e) advertising or offering consumer goods or services without intent to sell, lease, or rent them as advertised or offered; (f) deception, fraud, false pretense, false premise, misrepresentation, or knowing concealment, suppression, or omission of any material fact with the intent that a consumer rely on the same in connection with the promotion or sale of consumer goods or services or the subsequent performance with respect to an agreement, sale lease or rental.

584. Intel engaged in these unfair and deceptive trade practices in connection with offering for sale or selling consumer goods or services or with respect to the extension of consumer credit, in violation of Md. Comm. Code § 13-303.

585. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

586. Intel intended to mislead Plaintiff and Maryland Subclass members and induce them to rely on its misrepresentations and omissions.

587. Had Intel disclosed to Plaintiff and Subclass members material facts, including but not limited to, that in designing its CPUs, it failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks, and was otherwise engaged in deceptive, common business practices, Intel would have been unable to continue in business and it would have been forced to disclose the uniform Defects in its CPUs. Instead, Intel represented that its CPUs were continually improving in speed and performed better than other processors on the market. Plaintiff and the Subclass members acted reasonably in relying on Intel's misrepresentations and omissions, the truth of which they could not have discovered.

588. Intel acted intentionally, knowingly, and maliciously to violate Maryland's Consumer Protection Act, and recklessly disregarded Plaintiff and Maryland Subclass members' rights. Intel's knowledge of the CPUs' security and performance issues put it on notice that the CPUs were not as it advertised.

589. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiff and Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues.

590. Plaintiff and Maryland Subclass members seek all monetary and non-monetary relief allowed by law, including damages, disgorgement, injunctive relief, and attorneys' fees and costs.

MICHIGAN SUBCLASS COUNT XXXII

MICHIGAN CONSUMER PROTECTION ACT,
Mich. Comp. Laws Ann. §§ 445.903, *et seq.*

591. The Michigan Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Michigan Subclass, repeats and re-alleges all previously alleged paragraphs, as if fully alleged herein.

592. Intel and Michigan Subclass members are "persons" as defined by Mich. Comp. Laws Ann. § 445.903(d).

593. Intel advertised, offered, or sold goods or services in Michigan and engaged in trade or commerce directly or indirectly affecting the people of Michigan, as defined by Mich. Comp. Laws Ann. § 445.903(g).

594. Intel engaged in unfair, unconscionable, and deceptive practices in the conduct of trade and commerce, in violation of Mich. Comp. Laws Ann. § 445.903(1), including: (a) representing that its goods and services have characteristics, uses, and benefits that they do not have, in violation of Mich. Comp. Laws Ann. § 445.903(1)(c); (b) representing that its goods and services are of a particular standard or quality if they are of another in violation of Mich. Comp. Laws Ann. § 445.903(1)(e); (c) making a representation or statement of fact material to the transaction such that a person reasonably believes the represented or suggested state of affairs to be other than it actually is, in violation of Mich. Comp. Laws Ann. § 445.903(1)(bb); and (d) failing to reveal facts that are material to the transaction in light of representations of fact made in a positive matter, in violation of Mich. Comp. Laws Ann. § 445.903(1)(cc).

595. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

596. Intel intended to mislead Plaintiff and Michigan Subclass members and induce them to rely on its misrepresentations and omissions.

597. Intel acted intentionally, knowingly, and maliciously to violate Michigan's Consumer Protection Act, and recklessly disregarded Plaintiff and Michigan Subclass members' rights. Intel's knowledge of the CPUs' security and performance issues put it on notice that the CPUs were not as it advertised.

598. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiff and Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues.

599. Plaintiff and Michigan Subclass members seek all monetary and non-monetary relief allowed by law, including the greater of actual damages or $250, injunctive relief, and any other relief that is just and proper.

MINNESOTA SUBCLASS COUNT XXXIII

MINNESOTA CONSUMER FRAUD ACT,
Minn. Stat. §§ 325F.68, *et seq.* and Minn. Stat. §§ 8.31, *et seq.*

600. The Minnesota Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Minnesota Subclass, repeats and re-alleges all previously alleged paragraphs, as if fully alleged herein.

601. Intel, Plaintiff, and members of the Minnesota Subclass are each a "person" as defined by Minn. Stat. § 325F.68(3).

602. Intel goods, services, commodities, and intangibles (specifically, its CPUs) are "merchandise" as defined by Minn. Stat. § 325F.68(2).

603. Intel engaged in "sales" as defined by Minn. Stat. § 325F.68(4).

604. Intel engaged in fraud, false pretense, false promise, misrepresentation, misleading statements, and deceptive practices in connection with the sale of merchandise, in violation of Minn. Stat. § 325F.69(1), as described herein.

605. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

606. Intel intended to mislead Plaintiff and Minnesota Subclass members and induce them to rely on its misrepresentations and omissions.

607. Intel's fraudulent, misleading, and deceptive practices affected the public interest, including millions of Minnesotans who purchased and/or used Intel CPUs.

608. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiff and Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues.

609. Plaintiff and Minnesota Subclass members seek all monetary and non-monetary relief allowed by law, including damages, injunctive or other equitable relief, and attorneys' fees, disbursements, and costs.

MINNESOTA SUBCLASS COUNT XXXIV

MINNESOTA UNIFORM DECEPTIVE TRADE PRACTICES ACT,
Minn. Stat. §§ 325D.43, *et seq.*

610. The Minnesota Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Minnesota Subclass, repeats and re-alleges all previously alleged paragraphs, as if fully alleged herein.

611. By engaging in deceptive trade practices in the course of its business and vocation, directly or indirectly affecting the people of Minnesota, Intel violated Minn. Stat. § 325D.44, including the following provisions: representing that its goods and services had characteristics, uses, and benefits that they did not have, in violation of Minn. Stat. § 325D.44(1)(5); representing that goods and services are of a particular standard or quality when they are of another, in violation of Minn. Stat. § 325D.44(1)(7); advertising goods and services with intent not to sell them as advertised, in violation of Minn. Stat. § 325D.44(1)(9); and engaging in other conduct which similarly creates a likelihood of confusion or misunderstanding, in violation of Minn. Stat. § 325D.44(1)(13).

612. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

613. Intel intended to mislead Plaintiff and Minnesota Subclass members and induce them to rely on its misrepresentations and omissions.

614. Had Intel disclosed to Plaintiff and Subclass members material facts, including but not limited to, that in designing its CPUs, it failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks, and was otherwise engaged in deceptive, common business practices, Intel would have been unable to continue in business and it would have been forced to disclose the uniform Defects in its CPUs. Instead, Intel represented that its CPUs were continually improving in speed and performed better than other processors on the market. Plaintiff and the Subclass members acted reasonably in relying on Intel's misrepresentations and omissions, the truth of which they could not have discovered.

615. Intel acted intentionally, knowingly, and maliciously to violate Minnesota's Uniform Deceptive Trade Practices Act, and recklessly disregarded Plaintiff and Minnesota Subclass members' rights. Intel's knowledge of the CPUs' security and performance issues put it on notice that the CPUs were not as it advertised.

616. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiff and Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues.

617. Plaintiff and Minnesota Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief and attorneys' fees and costs.

MISSISSIPPI SUBCLASS COUNT XXXV

MISSISSIPPI CONSUMER PROTECTION ACT,
Miss. Code §§ 75-24-1, *et seq.*

618. The Mississippi Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Mississippi Subclass, repeats and re-alleges all previously alleged paragraphs, as if fully alleged herein.

619. Intel is a "person," as defined by Miss. Code § 75-24-3.

620. Intel advertised, offered, or sold goods or services in Mississippi and engaged in trade or commerce directly or indirectly affecting the people of Mississippi, as defined by Miss. Code § 75-24-3.

621. Prior to filing suit, Plaintiff made reasonable attempts to resolve Plaintiff's claims via informal dispute resolution processes; however, such processes were unsuccessful.

622. The above-described conduct violated Miss. Code Ann. § 75-24-5(2), including: representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that they do not have; representing that goods or services are of a particular standard, quality, or grade, or that goods are of a particular style or model, if they are of another; and advertising goods or services with intent not to sell them as advertised.

623. Intel intended to mislead Plaintiff and Mississippi Subclass members and induce them to rely on its misrepresentations and omissions.

624. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

625. Had Intel disclosed to Plaintiff and Subclass members material facts, including but not limited to, that in designing its CPUs, it failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks, and was otherwise engaged in deceptive, common business practices, Intel would have been unable to continue in business and it would have been forced to disclose the uniform Defects in its CPUs. Instead, Intel represented that its CPUs were continually improving in speed and performed better than other processors on the market. Plaintiff and the Subclass members acted reasonably in relying on Intel's misrepresentations and omissions, the truth of which they could not have discovered.

626. Intel had a duty to disclose the above-described facts due to the circumstances of this case. Intel duty to disclose arose from its: possession of exclusive knowledge regarding the Defects in its CPUs; active concealment of the Defects in its CPUs; and incomplete representations about its CPUs, security, and performance.

627. Intel acted intentionally, knowingly, and maliciously to violate Mississippi's Consumer Protection Act, and recklessly disregarded Plaintiff and Mississippi Subclass members' rights. Intel's knowledge of the CPUs' security and performance issues put it on notice that the CPUs were not as it advertised.

628. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiff and Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues.

629. Intel's violations present a continuing risk to Plaintiff and Mississippi Subclass members as well as to the general public as, *inter alia*, its omissions and misrepresentations have not been corrected.

630. Plaintiff and Mississippi Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, restitution and other relief under Miss. Code § 75-24-11, injunctive relief, punitive damages, and reasonable attorneys' fees and costs.

MISSOURI SUBCLASS COUNT XXXVI

MISSOURI MERCHANDISE PRACTICES ACT,
Mo. Rev. Stat. §§ 407.010, *et seq.*

631. The Missouri Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Missouri Subclass, repeats and re-alleges all previously alleged paragraphs, as if fully alleged herein.

632. Intel is a "person" as defined by Mo. Rev. Stat. § 407.010(5).

633. Intel advertised, offered, or sold goods or services in Missouri and engaged in trade or commerce directly or indirectly affecting the people of Missouri, as defined by Mo. Rev. Stat. § 407.010(4), (6) and (7).

634. Plaintiff and Missouri Subclass members purchased or leased goods or services primarily for personal, family, or household purposes.

635. Intel engaged in unlawful, unfair, and deceptive acts and practices, in connection with the sale or advertisement of merchandise in trade or commerce, in violation of Mo. Rev. Stat. § 407.020(1), as described herein.

636. Intel representations and omissions were material because they were likely to deceive reasonable consumers.

637. Intel intended to mislead Plaintiff and Missouri Subclass members and induce them to rely on its misrepresentations and omissions.

638. Intel acted intentionally, knowingly, and maliciously to violate Missouri's Merchandise Practices Act, and recklessly disregarded Plaintiff and Missouri Subclass members' rights. Intel's knowledge of the CPUs' security and performance issues put it on notice that the CPUs were not as it advertised.

639. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiff and Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues.

640. Plaintiff and Missouri Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, punitive damages, attorneys' fees and costs, injunctive relief, and any other appropriate relief.

MONTANA SUBCLASS COUNT XXXVII

MONTANA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION ACT, M.C.A. §§ 30-14-101, *et seq.*

641. The Montana Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Montana Subclass, repeats and re-alleges all previously alleged paragraphs, as if fully alleged herein.

642. Intel is a "person" as defined by MCA § 30-14-102(6).

643. Plaintiff and Montana Subclass members are "consumers" as defined by M.C.A. § 30-14-102(1).

644. Intel advertised, offered, or sold goods or services in Montana and engaged in trade or commerce directly or indirectly affecting the people of Montana, as defined by M.C.A. § 30-14-102(8).

645. Intel engaged in unfair and deceptive acts and practices in the conduct of trade or commerce, in violation M.C.A. § 30-14-103, as described herein.

646. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

647. Had Intel disclosed to Plaintiff and Subclass members material facts, including but not limited to, that in designing its CPUs, it failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks, and was otherwise engaged in deceptive, common business practices, Intel would have been unable to continue in business and it would have been forced to disclose the uniform Defects in its CPUs. Instead, Intel represented that its CPUs were continually improving in speed and performed better than other processors on the market. Plaintiff and the Subclass members acted reasonably in relying on Intel's misrepresentations and omissions, the truth of which they could not have discovered.

648. Intel's acts described above are unfair and offend public policy; they are immoral, unethical, oppressive, unscrupulous, and substantially injurious to consumers.

649. Intel acted intentionally, knowingly, and maliciously to violate Montana's Unfair Trade Practices and Consumer Protection Act, and recklessly disregarded Plaintiff and Montana Subclass members' rights. Intel's knowledge of the CPUs' security and performance issues put it on notice that the CPUs were not as it advertised.

650. As a direct and proximate result of Intel's unfair methods of competition and unfair and deceptive acts and practices in the conduct of trade or commerce, Plaintiff and Montana Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues.

651. Plaintiff and Montana Subclass members seek all monetary and non-monetary relief allowed by law, including the greater of (a) actual damages or (b) statutory damages of $500, treble damages, restitution, attorneys' fees and costs, injunctive relief, and other relief that the Court deems appropriate.

NEBRASKA SUBCLASS COUNT XXXVIII

NEBRASKA CONSUMER PROTECTION ACT,
Neb. Rev. Stat. §§ 59-1601, *et seq.*

652. The Nebraska Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Nebraska Subclass, repeats and re-alleges all previously alleged paragraphs, as if fully alleged herein.

653. Intel and Nebraska Subclass members are each a "person" as defined by Neb. Rev. Stat. § 59-1601(1).

654. Intel advertised, offered, or sold goods or services in Nebraska and engaged in trade or commerce directly or indirectly affecting the people of Nebraska, as defined by Neb. Rev. Stat. § 59-1601.

655. Intel engaged in unfair and deceptive acts and practices in conducting trade and commerce, in violation of Neb. Rev. Stat. § 59-1602, as described herein.

656. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

657. As a direct and proximate result of Intel's unfair and deceptive acts and practices, Plaintiff and Nebraska Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues.

658. Intel's unfair and deceptive acts and practices complained of herein affected the public interest, including the large percentage of Nebraskans who have purchased and/or used Intel CPUs.

659. Plaintiff and Nebraska Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief, the greater of either (1) actual damages or (2) $1,000, civil penalties, and reasonable attorneys' fees and costs.

NEBRASKA SUBCLASS COUNT XXIX

NEBRASKA UNIFORM DECEPTIVE TRADE PRACTICES ACT, Neb. Rev. Stat. §§ 87-301, *et seq.*

660. The Nebraska Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Nebraska Subclass, repeats and re-alleges all previously alleged paragraphs, as if fully alleged herein.

661. Intel and Nebraska Subclass members are "persons" as defined by Neb. Rev. Stat. § 87-301(19).

662. Intel advertised, offered, or sold goods or services in Nebraska and engaged in trade or commerce directly or indirectly affecting the people of Nebraska.

663. Intel engaged in deceptive trade practices in the course of its business, in violation of Neb. Rev. Stat. §§ 87-302(a)(5), (8), and (10), including: represented that goods and services have characteristics, uses, benefits, or qualities that they do not have; represented that goods and services are of a particular standard, quality, or grade if they are of another; and advertised its goods and services with intent not to sell them as advertised and in a manner calculated or tending to mislead or deceive.

664. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

665. Intel intended to mislead Plaintiff and Nebraska Subclass members and induce them to rely on its misrepresentations and omissions.

666. Had Intel disclosed to Plaintiff and Subclass members material facts, including but not limited to, that in designing its CPUs, it failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks, and was otherwise engaged in deceptive, common business practices, Intel would have been unable to continue in business and it would have been forced to disclose the uniform Defects in its CPUs. Instead, Intel represented that its CPUs were continually improving in speed and performed better than other processors on the market. Plaintiff and the Subclass members acted reasonably in relying on Intel's misrepresentations and omissions, the truth of which they could not have discovered.

667. Intel acted intentionally, knowingly, and maliciously to violate Nebraska's Uniform Deceptive Trade Practices Act, and recklessly disregarded Plaintiff and Nebraska Subclass members' rights. Intel's knowledge of the CPUs' security and performance issues put it on notice that the CPUs were not as it advertised.

668. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiff and Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues.

669. Intel's deceptive trade practices complained of herein affected consumers at large, including the large percentage of Nebraskans who purchased and/or used Intel CPUs.

670. Plaintiff and Nebraska Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief, other equitable relief, civil penalties, and attorneys' fees and costs.

NEVADA SUBCLASS COUNT XL

NEVADA DECEPTIVE TRADE PRACTICES ACT,
Nev. Rev. Stat. Ann. §§ 598.0903, *et seq.*

671. The Nevada Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Nevada Subclass, repeats and re-alleges all previously alleged paragraphs, as if fully alleged herein.

672. Intel advertised, offered, or sold goods or services in Nevada and engaged in trade or commerce directly or indirectly affecting the people of Nevada.

673. Intel engaged in deceptive trade practices in the course of its business or occupation, in violation of Nev. Rev. Stat. §§ 598.0915 and 598.0923, including: knowingly making a false representation as to the characteristics, uses, and benefits of goods or services for sale in violation of Nev. Rev. Stat. § 598.0915(5); representing that goods or services for sale are of a particular standard, quality, or grade when Intel knew or should have known that they are of another standard, quality, or grade in violation of Nev. Rev. Stat. § 598.0915(7); advertising goods

or services with intent not to sell them as advertised in violation of Nev. Rev. Stat § 598.0915(9); failing to disclose a material fact in connection with the sale of goods or services in violation of Nev. Rev. Stat. § 598.0923(A)(2); and violating state and federal statutes or regulations relating to the sale of goods or services in violation of Nev. Rev. Stat. § 598.0923(A)(3).

674. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

675. Had Intel disclosed to Plaintiff and Subclass members material facts, including but not limited to, that in designing its CPUs, it failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks, and was otherwise engaged in deceptive, common business practices, Intel would have been unable to continue in business and it would have been forced to disclose the uniform Defects in its CPUs. Instead, Intel represented that its CPUs were continually improving in speed and performed better than other processors on the market. Plaintiff and the Subclass members acted reasonably in relying on Intel's misrepresentations and omissions, the truth of which they could not have discovered.

676. Intel acted intentionally, knowingly, and maliciously to violate Nevada's Deceptive Trade Practices Act, and recklessly disregarded Plaintiff and Nevada Subclass members' rights. Intel's knowledge of the CPUs' security and performance issues put it on notice that the CPUs were not as it advertised.

677. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiff and Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of

their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues.

678. Plaintiff and Nevada Subclass members seek all monetary and non-monetary relief allowed by law, including damages, punitive damages, and attorneys' fees and costs.

NEW HAMPSHIRE SUBCLASS COUNT XLI

NEW HAMPSHIRE CONSUMER PROTECTION ACT,
N.H.R.S.A. §§ 358-A, *et seq.*

679. The New Hampshire Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the New Hampshire Subclass, repeats and re-alleges all previously alleged paragraphs, as if fully alleged herein.

680. Intel is a "person" under the New Hampshire Consumer Protection statute.

681. Intel advertised, offered, or sold goods or services in New Hampshire and engaged in trade or commerce directly or indirectly affecting the people of New Hampshire, as defined by N.H.R.S.A. § 358-A:1.

682. Intel engaged in unfair and deceptive acts or practices in the ordinary conduct of its trade or business, in violation of N.H.R.S.A. § 358-A:2, including: representing that its goods or services have characteristics, uses, or benefits that they do not have in violation of N.H.R.S.A. § 358-A:2.V; representing that its goods or services are of a particular standard or quality if they are of another in violation of N.H.R.S.A. § 358-A:2.VII; and advertising its goods or services with intent not to sell them as advertised in violation of N.H.R.S.A. § 358-A:2.IX.

683. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

684. Intel acted intentionally, knowingly, and maliciously to violate New Hampshire's Consumer Protection Act, and recklessly disregarded Plaintiff and New Hampshire Subclass

members' rights. Intel's knowledge of the CPUs' security and performance issues put it on notice that the CPUs were not as it advertised. Intel's acts and practices went beyond the realm of strictly private transactions.

685. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiff and Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues.

686. Plaintiff and New Hampshire Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, punitive damages, equitable relief (including injunctive relief), restitution, civil penalties, and attorneys' fees and costs.

NEW JERSEY SUBCLASS COUNT XLII

NEW JERSEY CONSUMER FRAUD ACT,
N.J. Stat. Ann. §§ 56:8-1, *et seq.*

687. The New Jersey Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the New Jersey Subclass, repeats and re-alleges all previously alleged paragraphs, as if fully alleged herein.

688. Intel is a "person," as defined by N.J. Stat. Ann. § 56:8-1(d).

689. Intel sells "merchandise," as defined by N.J. Stat. Ann. § 56:8-1(c) & (e).

690. The New Jersey Consumer Fraud Act, N.J. Stat. §§ 56:8-1, *et seq.*, prohibits unconscionable commercial practices, deception, fraud, false pretense, false promise, misrepresentation, as well as the knowing concealment, suppression, or omission of any material fact with the intent that others rely on the concealment, omission, or fact, in connection with the sale or advertisement of any merchandise.

691. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

692. Intel intended to mislead Plaintiff and New Jersey Subclass members and induce them to rely on its misrepresentations and omissions.

693. Intel acted intentionally, knowingly, and maliciously to violate New Jersey's Consumer Fraud Act, and recklessly disregarded Plaintiff and New Jersey Subclass members' rights. Intel's knowledge of the CPUs' security and performance issues put it on notice that the CPUs were not as it advertised.

694. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiff and Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues.

695. Plaintiff and New Jersey Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief, other equitable relief, actual damages, treble damages, restitution, and attorneys' fees, filing fees, and costs.

NEW MEXICO SUBCLASS COUNT XLIII

NEW MEXICO UNFAIR PRACTICES ACT,
N.M. Stat. Ann. §§ 57-12-2, *et seq.*

696. The New Mexico Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the New Mexico Subclass, repeats and re-alleges all previously alleged paragraphs, as if fully alleged herein.

697. Intel is a "person" as meant by N.M. Stat. Ann. § 57-12-2.

698. Intel was engaged in "trade" and "commerce" as meant by N.M. Stat. Ann. § 57-12-2(C) when engaging in the conduct alleged.

699. The New Mexico Unfair Practices Act, N.M. Stat. Ann. §§ 57-12-2, *et seq.*, prohibits both unfair or deceptive trade practices and unconscionable trade practices in the conduct of any trade or commerce.

700. Intel engaged in unconscionable, unfair, and deceptive acts and practices in connection with the sale of goods or services in the regular course of its trade or commerce, including the following: knowingly representing that its goods and services have characteristics, benefits, or qualities that they do not have, in violation of N.M. Stat. Ann. § 57-12-2(D)(5); knowingly representing that its goods and services are of a particular standard or quality when they are of another in violation of N.M. Stat. Ann. § 57-12-2(D)(7); knowingly using exaggeration, innuendo, or ambiguity as to a material fact or failing to state a material fact where doing so deceives or tends to deceive in violation of N.M. Stat. Ann. § 57-12-2(D)(14); taking advantage of the lack of knowledge, experience, or capacity of its consumers to a grossly unfair degree to Plaintiff's and the New Mexico Subclass' detriment in violation of N.M. Stat. Ann. § 57-2-12(E)(1); and performing these acts and practices in a way that results in a gross disparity between the value received by Plaintiff and the New Mexico Subclass and the price paid, to their detriment, in violation of N.M. Stat. § 57-2-12(E)(2).

701. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

702. Intel intended to mislead Plaintiff and New Mexico Subclass members and induce them to rely on its misrepresentations and omissions.

703. Intel acted intentionally, knowingly, and maliciously to violate New Mexico's Unfair Practices Act, and recklessly disregarded Plaintiff and New Mexico Subclass members' rights. Intel's knowledge of the CPUs' security and performance issues put it on notice that the CPUs were not as it advertised.

704. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiff and Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues.

705. Plaintiff and New Mexico Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief, actual damages or statutory damages of $100 (whichever is greater), treble damages or statutory damages of $300 (whichever is greater), and reasonable attorneys' fees and costs.

NEW YORK SUBCLASS COUNT XLIV

NEW YORK GENERAL BUSINESS LAW, N.Y. Gen. Bus. Law §§ 349, *et seq.*

706. The New York Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the New York Subclass, repeats and re-alleges all previously alleged paragraphs, as if fully alleged herein.

707. Intel engaged in deceptive acts or practices in the conduct of its business, trade, and commerce or furnishing of services, in violation of N.Y. Gen. Bus. Law § 349, as described herein.

708. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

709. Intel acted intentionally, knowingly, and maliciously to violate New York's General Business Law, and recklessly disregarded Plaintiff and New York Subclass members' rights. Intel's knowledge of the CPUs' security and performance issues put it on notice that the CPUs were not as it advertised.

710. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiff and Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues.

711. Intel's deceptive and unlawful acts and practices complained of herein affected the public interest and consumers at large, including the millions of New Yorkers who purchased and/or used Intel CPUs.

712. The above deceptive and unlawful practices and acts by Intel caused substantial injury to Plaintiff and New York Subclass members that they could not reasonably avoid.

713. Plaintiff and New York Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of $50 (whichever is greater), treble damages, injunctive relief, and attorney's fees and costs.

<u>NORTH CAROLINA SUBCLASS COUNT XLV</u>

NORTH CAROLINA UNFAIR TRADE PRACTICES ACT,
N.C. Gen. Stat. Ann. §§ 75-1.1, *et seq.*

714. The North Carolina Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the North Carolina Subclass, repeats and re-alleges all previously alleged paragraphs, as if fully alleged herein.

715. Intel advertised, offered, or sold goods or services in North Carolina and engaged in trade or commerce directly or indirectly affecting the people of North Carolina, as defined by N.C. Gen. Stat. Ann. § 75-1.1(b).

716. Intel engaged in unfair and deceptive acts and practices in or affecting commerce, in violation of N.C. Gen. Stat. Ann. § 75-1.1, as described herein.

717. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

718. Intel intended to mislead Plaintiff and North Carolina Subclass members and induce them to rely on its misrepresentations and omissions.

719. Had Intel disclosed to Plaintiff and Subclass members material facts, including but not limited to, that in designing its CPUs, it failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks, and was otherwise engaged in deceptive, common business practices, Intel would have been unable to continue in business and it would have been forced to disclose the uniform Defects in its CPUs. Instead, Intel represented that its CPUs were continually improving in speed and performed better than other processors on the market. Plaintiff and the Subclass members acted reasonably in relying on Intel's misrepresentations and omissions, the truth of which they could not have discovered.

720. Intel acted intentionally, knowingly, and maliciously to violate North Carolina's Unfair Trade Practices Act, and recklessly disregarded Plaintiff and North Carolina Subclass members' rights. Intel's knowledge of the CPUs' security and performance issues put it on notice that the CPUs were not as it advertised.

721. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiff and Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues.

722. Intel's conduct as alleged herein was continuous, such that after the first violations of the provisions pled herein, each week that the violations continued constitute separate offenses pursuant to N.C. Gen. Stat. Ann. § 75-8.

723. Plaintiff and North Carolina Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, treble damages, and attorneys' fees and costs.

NORTH DAKOTA SUBCLASS COUNT XLVI

NORTH DAKOTA UNLAWFUL SALES OR ADVERTISING ACT,
N.D. Cent. Code §§ 51-15-01, *et seq.*

724. The North Dakota Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the North Dakota Subclass, repeats and re-alleges all previously alleged paragraphs, as if fully alleged herein.

725. Intel, Plaintiff, and each member of the North Dakota Subclass is a "person," as defined by N.D. Cent. Code § 51-15-01(4).

726. Intel sells and advertises "merchandise," as defined by N.D. Cent. Code § 51-15-01(3) and (5).

727. Intel advertised, offered, or sold goods or services in North Dakota and engaged in trade or commerce directly or indirectly affecting the people of North Dakota.

728. Intel engaged in deceptive, false, fraudulent, misrepresentative, unconscionable, and substantially injurious acts and practices in connection with the sale and advertisement of merchandise, in violation of N.D. Cent. Code § 51-15-01, as described herein.

729. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

730. Intel's above-described acts and practices caused substantial injury to Plaintiff and North Dakota Subclass members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

731. Intel intended to mislead Plaintiff and North Dakota Subclass members and induce them to rely on its misrepresentations and omissions.

732. Intel acted intentionally, knowingly, and maliciously to violate North Dakota's Unlawful Sales or Advertising Law, and recklessly disregarded Plaintiff and North Dakota Subclass members' rights. Intel's knowledge of the CPUs' security and performance issues put it on notice that the CPUs were not as it advertised.

733. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiff and Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues.

734. Plaintiff and North Dakota Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief, damages, restitution, treble damages, civil penalties, and attorneys' fees, costs, and disbursements.

OHIO SUBCLASS COUNT XLVII

OHIO CONSUMER SALES PRACTICES ACT,
Ohio Rev. Code §§ 1345.01, *et seq.*

735. The Ohio Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Ohio Subclass, repeats and re-alleges all previously alleged paragraphs, as if fully alleged herein.

736. Plaintiff and Ohio Subclass members are "persons," as defined by Ohio Rev. Code § 1345.01(B).

737. Intel was a "supplier" engaged in "consumer transactions," as defined by Ohio Rev. Code §§ 1345.01(A) & (C).

738. Intel advertised, offered, or sold goods or services in Ohio and engaged in trade or commerce directly or indirectly affecting the people of Ohio.

739. Intel engaged in unfair and deceptive acts and practices in connection with a consumer transaction, in violation of Ohio Rev. Code §§ 1345.02, including: representing that its goods, services, and intangibles had performance characteristics, uses, and benefits that it did not have, in violation of Ohio Rev. Code § 1345.02(B)(1); and representing that its goods, services, and intangibles were of a particular standard or quality when they were not, in violation of Ohio Rev. Code § 1345(B)(2).

740. Intel engaged in unconscionable acts and practices in connection with a consumer transaction, in violation of Ohio Rev. Code Ann. § 1345.03, including: knowingly taking advantage of the inability of Plaintiff and the Ohio Subclass to reasonably protect their interest because of their ignorance of the issues discussed herein (Ohio Rev. Code Ann. § 1345.03(B)(1)); and requiring Plaintiff and the Ohio Subclass to enter into a consumer transaction on terms that Intel knew were substantially one-sided in favor of Intel (Ohio Rev. Code Ann. § 1345.03(B)(5)).

741. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

742. Intel intended to mislead Plaintiff and Ohio Subclass members and induce them to rely on its misrepresentations and omissions.

743. Intel acted intentionally, knowingly, and maliciously to violate Ohio's Consumer Sales Practices Act, and recklessly disregarded Plaintiff and Ohio Subclass members' rights. Intel's knowledge of the CPUs' security and performance issues put it on notice that the CPUs were not as it advertised.

744. .Intel's unfair, deceptive, and unconscionable acts and practices complained of herein affected the public interest, including the millions of Ohioans who purchased and/or used Intel CPUs.

745. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiff and Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues.

746. Plaintiff and the Ohio Subclass members seek all monetary and non-monetary relief allowed by law, including declaratory and injunctive relief, the greater of actual and treble damages or statutory damages, attorneys' fees and costs, and any other appropriate relief.

OHIO SUBCLASS COUNT XLVIII

OHIO DECEPTIVE TRADE PRACTICES ACT,
Ohio Rev. Code §§ 4165.01, *et seq.*

747. The Ohio Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Ohio Subclass, repeats and re-alleges all previously alleged paragraphs, as if fully alleged herein.

748. Intel, Plaintiff, and Ohio Subclass members are a "person," as defined by Ohio Rev. Code § 4165.01(D).

749. Intel advertised, offered, or sold goods or services in Ohio and engaged in trade or commerce directly or indirectly affecting the people of Ohio.

750. Intel engaged in deceptive trade practices in the course of its business and vocation, in violation of Ohio Rev. Code § 4165.02, including: representing that its goods and services have characteristics, uses, benefits, or qualities that they do not have, in violation of Ohio Rev. Code § 4165.02(A)(7); representing that its goods and services are of a particular standard or quality when they are of another, in violation of Ohio Rev. Code § 4165.02(A)(9); and advertising its goods and services with intent not to sell them as advertise, in violation of Ohio Rev. Code § 4165.02(A)(11).

751. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

752. Intel intended to mislead Plaintiff and Ohio Subclass members and induce them to rely on its misrepresentations and omissions.

753. Intel acted intentionally, knowingly, and maliciously to violate Ohio's Deceptive Trade Practices Act, and recklessly disregarded Plaintiff and Ohio Subclass members' rights.

Intel's knowledge of the CPUs' security and performance issues put it on notice that the CPUs were not as it advertised.

754. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiff and Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues.

755. Plaintiff and Ohio Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief, actual damages, attorneys' fees, and any other relief that is just and proper.

OKLAHOMA SUBCLASS COUNT XLIX

OKLAHOMA CONSUMER PROTECTION ACT,
Okla. Stat. Tit. 15, §§ 751, *et seq.*

756. The Oklahoma Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Oklahoma Subclass, repeats and re-alleges all previously alleged paragraphs, as if fully alleged herein.

757. Intel is a "person," as meant by Okla. Stat. tit. 15, § 752(1).

758. Intel's advertisements, offers of sales, sales, and distribution of goods, services, and other things of value constituted "consumer transactions" as meant by Okla. Stat. tit. 15, § 752(2).

759. Intel, in the course of its business, engaged in unlawful practices in violation of Okla. Stat. tit. 15, § 753, including the following: making false representations, knowingly or with reason to know, as to the characteristics, uses, and benefits of the subjects of its consumer transactions, in violation of Okla. Stat. tit. 15, § 753(5); representing, knowingly or with reason to know, that the subjects of its consumer transactions were of a particular standard when they were

of another, in violation of Okla. Stat. tit 15, § 753(7); advertising, knowingly or with reason to know, the subjects of its consumer transactions with intent not to sell as advertised, in violation of Okla. Stat. tit 15, § 753 (8); committing unfair trade practices that offend established public policy and was immoral, unethical, oppressive, unscrupulous, and substantially injurious to consumers as defined by section 752(14), in violation of Okla. Stat. tit. 15, § 753(20); and committing deceptive trade practices that deceived or could reasonably be expected to deceive or mislead a person to the detriment of that person as defined by section 752(13), in violation of Okla. Stat. tit. 15, § 753(20).

760. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

761. Intel intended to mislead Plaintiff and Oklahoma Subclass members and induce them to rely on its misrepresentations and omissions.

762. Had Intel disclosed to Plaintiff and Subclass members material facts, including but not limited to, that in designing its CPUs, it failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks, and was otherwise engaged in deceptive, common business practices, Intel would have been unable to continue in business and it would have been forced to disclose the uniform Defects in its CPUs. Instead, Intel represented that its CPUs were continually improving in speed and performed better than other processors on the market. Plaintiff and the Subclass members acted reasonably in relying on Intel's misrepresentations and omissions, the truth of which they could not have discovered.

763. The above unlawful practices and acts by Intel were immoral, unethical, oppressive, unscrupulous, and substantially injurious. These acts caused substantial injury to Plaintiff and Oklahoma Subclass members.

764. Intel acted intentionally, knowingly, and maliciously to violate Oklahoma's Consumer Protection Act, and recklessly disregarded Plaintiff and Oklahoma Subclass members' rights. Intel's knowledge of the CPUs' security and performance issues put it on notice that the CPUs were not as it advertised.

765. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiff and Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues.

766. Plaintiff and Oklahoma Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, civil penalties, and attorneys' fees and costs.

OREGON SUBCLASS COUNT L

OREGON UNLAWFUL TRADE PRACTICES ACT,
Or. Rev. Stat. §§ 646.608, *et seq.*

767. The Oregon Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Oregon Subclass, repeats and re-alleges all previously alleged paragraphs, as if fully alleged herein.

768. Intel is a "person," as defined by Or. Rev. Stat. § 646.605(4).

769. Intel engaged in the sale of "goods and services," as defined by Or. Rev. Stat. § 646.605(6)(a).

770. Intel sold "goods or services," as defined by Or. Rev. Stat. § 646.605(6)(a).

771. Intel advertised, offered, or sold goods or services in Oregon and engaged in trade or commerce directly or indirectly affecting the people of Oregon.

772. Intel engaged in unlawful practices in the course of its business and occupation, in violation of Or. Rev. Stat. § 646.608, included the following: representing that its goods and services have approval, characteristics, uses, benefits, and qualities that they do not have, in violation of Or. Rev. Stat. § 646.608(1)(e); representing that its goods and services are of a particular standard or quality if they are of another, in violation of Or. Rev. Stat. § 646.608(1)(g); advertising its goods or services with intent not to provide them as advertised, in violation of Or. Rev. Stat. § 646.608(1)(i); and concurrent with tender or delivery of its goods and services, failing to disclose any known material Defect, in violation of Or. Rev. Stat. § 646.608(1)(t).

773. Intel's representations and omissions were material because they were likely to deceive reasonable consumers. Specifically, Intel's conduct included:

a. Knowingly designing, developing, manufacturing, advertising, and selling CPUs with significant Defects that result in security risks, compromising consumer data, and—if patched—slowing down the CPUs so that consumers did not receive the benefit of their bargain;

b. Marketing and selling Intel CPUs that relied upon speculative execution as a means to achieve higher speeds to compete in the CPU market, while at the same time exposing consumers to side-channel security threats solely to increase profits;

c. Permitting instruction execution in the Intel CPUs without first performing and enforcing the appropriate memory access checks as a means to increase processor speed and, accordingly, putting profits over the safety of consumer data;

d. Failing to take steps to secure the CPU architecture from cache side-channel attacks;

e. Making affirmative public representations about the security of Intel CPUs while, at the same time, not ensuring that safety is a priority in its devices;

f. Making affirmative public representations about the speed of Intel CPUs while knowing that, for those CPUs to offer security for consumer data, they would need to be patched, which would reduce processor speed or leave systems corrupted and still vulnerable; and

g. Concealing and/or failing to disclose material facts, including but not limited to, that in designing its CPUs, it failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks.

774. Intel intended to mislead Plaintiff and Oregon Subclass members and induce them to rely on its misrepresentations and omissions.

775. Had Intel disclosed to Plaintiff and Subclass members material facts, including but not limited to, that in designing its CPUs, it failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks, and was otherwise engaged in deceptive, common business practices, Intel would have been unable to continue in business and it would have been forced to disclose the uniform Defects in its CPUs. Instead, Intel represented that its CPUs were continually improving in speed and performed better than other processors on the market. Plaintiff and the Subclass members acted reasonably in relying on Intel's misrepresentations and omissions, the truth of which they could not have discovered.

776. Intel acted intentionally, knowingly, and maliciously to violate Oregon's Unlawful Trade Practices Act, and recklessly disregarded Plaintiff and Oregon Subclass members' rights.

Intel's knowledge of the CPUs' security and performance issues put it on notice that the CPUs were not as it advertised.

777. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiff and Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues.

778. Plaintiff and Oregon Subclass members seek all monetary and non-monetary relief allowed by law, including equitable relief, actual damages or statutory damages of $200 per violation (whichever is greater), punitive damages, and reasonable attorneys' fees and costs.

PENNSYLVANIA SUBCLASS COUNT LI

PENNSYLVANIA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION LAW, 73 Pa. Cons. Stat. §§ 201-2 & 201-3, *et seq.*

779. The Pennsylvania Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Pennsylvania Subclass, repeats and re-alleges all previously alleged paragraphs, as if fully alleged herein.

780. Intel is a "person," as meant by 73 Pa. Cons. Stat. § 201-2(2).

781. Plaintiff and Pennsylvania Subclass members purchased goods and services in "trade" and "commerce," as meant by 73 Pa. Cons. Stat. § 201-2(3), primarily for personal, family, and/or household purposes.

782. Intel engaged in unfair methods of competition and unfair or deceptive acts or practices in the conduct of its trade and commerce in violation of 73 Pa. Cons. Stat. Ann. § 201-3, including the following: representing that its goods and services have characteristics, uses,

benefits, and qualities that they do not have (73 Pa. Stat. Ann. § 201-2(4)(v)); representing that its goods and services are of a particular standard or quality if they are another (73 Pa. Stat. Ann. § 201-2(4)(vii)); and advertising its goods and services with intent not to sell them as advertised (73 Pa. Stat. Ann. § 201-2(4)(ix)).

783. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

784. Intel intended to mislead Plaintiff and Pennsylvania Subclass members and induce them to rely on its misrepresentations and omissions.

785. Had Intel disclosed to Plaintiff and Subclass members material facts, including but not limited to, that in designing its CPUs, it failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks, and was otherwise engaged in deceptive, common business practices, Intel would have been unable to continue in business and it would have been forced to disclose the uniform Defects in its CPUs. Instead, Intel represented that its CPUs were continually improving in speed and performed better than other processors on the market. Plaintiff and the Subclass members acted reasonably in relying on Intel's misrepresentations and omissions, the truth of which they could not have discovered.

786. Intel acted intentionally, knowingly, and maliciously to violate Pennsylvania Unfair Trade Practices and Consumer Protection Law, and recklessly disregarded Plaintiff and Pennsylvania Subclass members' rights. Intel's knowledge of the CPUs' security and performance issues put it on notice that the CPUs were not as it advertised.

787. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiff and Subclass members have suffered and will continue to suffer injury, ascertainable losses of money

or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues.

788. Plaintiff and Pennsylvania Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of $100 (whichever is greater), treble damages, attorneys' fees and costs, and any additional relief the Court deems necessary or proper.

RHODE ISLAND SUBCLASS COUNT LII

RHODE ISLAND DECEPTIVE TRADE PRACTICES ACT,
R.I. Gen. Laws §§ 6-13.1, *et seq.*

789. The Rhode Island Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Rhode Island Subclass, repeats and re-alleges all previously alleged paragraphs, as if fully alleged herein.

790. Plaintiff and Rhode Island Subclass members are each a "person," as defined by R.I. Gen. Laws § 6-13.1-1(3).

791. Plaintiff and Rhode Island Subclass members purchased goods and services for personal, family, or household purposes.

792. Intel advertised, offered, or sold goods or services in Rhode Island and engaged in trade or commerce directly or indirectly affecting the people of Rhode Island, as defined by R.I. Gen. Laws § 6-13.1-1(5).

793. Intel engaged in unfair and deceptive acts and practices, in violation of R.I. Gen. Laws § 6-13.1-2, including: representing that its goods and services have characteristics, uses, and benefits that they do not have (R.I. Gen. Laws § 6-13.1-52(6)(v)); representing that its goods and services are of a particular standard or quality when they are of another (R.I. Gen. Laws § 6-13.1-

52(6)(vii)); advertising goods or services with intent not to sell them as advertised (R.I. Gen. Laws § 6-13.1-52(6)(ix)); engaging in any other conduct that similarly creates a likelihood of confusion or misunderstanding (R.I. Gen. Laws § 6-13.1-52(6)(xii)); engaging in any act or practice that is unfair or deceptive to the consumer (R.I. Gen. Laws § 6-13.1-52(6)(xiii)); and using other methods, acts, and practices that mislead or deceive members of the public in a material respect (R.I. Gen. Laws § 6-13.1-52(6)(xiv)).

794. Intel's representations and omissions were material because they were likely to deceive reasonable consumers. Specifically, Intel's actions included:

a. Knowingly designing, developing, manufacturing, advertising, and selling CPUs with significant Defects that result in security risks, compromising consumer data, and—if patched—slowing down the CPUs so that consumers did not receive the benefit of their bargain;

b. Marketing and selling Intel CPUs that relied upon speculative execution as a means to achieve higher speeds to compete in the CPU market, while at the same time exposing consumers to side-channel security threats solely to increase profits;

c. Permitting instruction execution in the Intel CPUs without first performing and enforcing the appropriate memory access checks as a means to increase processor speed and, accordingly, putting profits over the safety of consumer data;

d. Failing to take steps to secure the CPU architecture from cache side-channel attacks;

e. Making affirmative public representations about the security of Intel CPUs while, at the same time, not ensuring that safety is a priority in its devices;

f. Making affirmative public representations about the speed of Intel CPUs while knowing that, for those CPUs to offer security for consumer data, they would need to be patched, which would reduce processor speed or leave systems corrupted and still vulnerable; and

g. Concealing and/or failing to disclose material facts, including but not limited to, that in designing its CPUs, it failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks.

795. Intel intended to mislead Plaintiff and Rhode Island Subclass members and induce them to rely on its misrepresentations and omissions.

796. Intel acted intentionally, knowingly, and maliciously to violate Rhode Island's Deceptive Trade Practices Act, and recklessly disregarded Plaintiff and Rhode Island Subclass members' rights. Intel's knowledge of the CPUs' security and performance issues put it on notice that the CPUs were not as it advertised.

797. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiff and Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues.

798. Plaintiff and Rhode Island Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of $200 per Subclass Member (whichever is greater), punitive damages, injunctive relief, other equitable relief, and attorneys' fees and costs.

SOUTH CAROLINA SUBCLASS COUNT LIII

SOUTH CAROLINA UNFAIR TRADE PRACTICES ACT, S.C. Code Ann. §§ 39-5-10, *et seq.*

799. The South Carolina Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the South Carolina Subclass, repeats and re-alleges all previously alleged paragraphs, as if fully alleged herein.

800. Intel is a "person," as defined by S.C. Code Ann. § 39-5-10(a).

801. South Carolina's Unfair Trade Practices Act (SC UTPA) prohibits "unfair or deceptive acts or practices in the conduct of any trade or commerce." S.C. Code Ann. § 39-5-20.

802. Intel advertised, offered, or sold goods or services in South Carolina and engaged in trade or commerce directly or indirectly affecting the people of South Carolina, as defined by S.C. Code Ann. § 39-5-10(b).

803. Intel's acts and practices had, and continue to have, the tendency or capacity to deceive.

804. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

805. Intel intended to mislead Plaintiff and South Carolina Subclass members and induce them to rely on its misrepresentations and omissions.

806. Had Intel disclosed to Plaintiff and Subclass members material facts, including but not limited to, that in designing its CPUs, it failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks, and was otherwise engaged in deceptive, common business practices, Intel would have been unable to continue in business and it would have been forced to disclose the uniform Defects in its CPUs. Instead, Intel represented that its CPUs were continually improving in speed

and performed better than other processors on the market. Plaintiff and the Subclass members acted reasonably in relying on Intel's misrepresentations and omissions, the truth of which they could not have discovered.

807. Intel had a duty to disclose the above-described facts due to the circumstances of this case. Intel's duty to disclose also arose from its: possession of exclusive knowledge regarding the Defects in its CPUs and incomplete representations about the CPUs, while purposefully withholding material facts from Plaintiff and the South Carolina Subclass that contradicted these representations.

808. Intel's business acts and practices offend an established public policy, or are immoral, unethical, or oppressive.

809. Intel's unfair and deceptive acts or practices adversely affected the public interest because such acts or practices have the potential for repetition; Intel engages in such acts or practices as a general rule; and such acts or practices impact the public at large, including millions of South Carolina Subclass members that purchased and/or used an Intel CPU.

810. Intel unfair and deceptive acts or practices have the potential for repetition because the same kinds of actions occurred in the past, as described herein, thus making it likely that these acts or practices will continue to occur if left undeterred. Additionally, Intel's policies and procedures create the potential for recurrence of the complained-of business acts and practices.

811. Intel violations present a continuing risk to Plaintiff and South Carolina Subclass members as well as to the general public.

812. Intel intended to mislead Plaintiff and South Carolina Subclass members and induce them to rely on its misrepresentations and omissions.

813. Intel acted intentionally, knowingly, and maliciously to violate South Carolina's Unfair Trade Practices Act, and recklessly disregarded Plaintiff and South Carolina Subclass members' rights. Intel's knowledge of the CPUs' security and performance issues put it on notice that the CPUs were not as it advertised. In light of this conduct, punitive damages would serve the interest of society in punishing and warning others not to engage in such conduct and would deter Intel and others from committing similar conduct in the future.

814. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiff and Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues.

815. Plaintiff and South Carolina Subclass members seek all monetary and non-monetary relief allowed by law, including damages for their economic losses, treble damages, punitive damages, injunctive relief, and reasonable attorneys' fees and costs.

SOUTH DAKOTA SUBCLASS COUNT LIV

SOUTH DAKOTA DECEPTIVE TRADE PRACTICES AND CONSUMER PROTECTION ACT, S.D. Codified Laws §§ 37-24-1, *et seq.*

816. The South Dakota Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the South Dakota Subclass, repeats and re-alleges all previously alleged paragraphs, as if fully alleged herein.

817. Intel is a "person," as defined by S.D. Codified Laws § 37-24-1(8).

818. Intel advertises and sells "merchandise," as defined by S.D. Codified Laws § 37-24-1(6), (7), & (13).

819. Intel advertised, offered, or sold goods or services in South Dakota and engaged in trade or commerce directly or indirectly affecting the people of South Dakota, as defined by S.D. Codified Laws § 37-24-1(6), (7), & (13).

820. Intel knowingly engaged in deceptive acts or practices, misrepresentation, concealment, suppression, or omission of material facts in connection with the sale and advertisement of goods or services, in violation of S.D. Codified Laws § 37-24-6, as described herein.

821. Intel intended to mislead Plaintiff and South Dakota Subclass members and induce them to rely on its misrepresentations and omissions.

822. Intel representations and omissions were material because they were likely to deceive reasonable consumers.

823. Had Intel disclosed to Plaintiff and Subclass members material facts, including but not limited to, that in designing its CPUs, it failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks, and was otherwise engaged in deceptive, common business practices, Intel would have been unable to continue in business and it would have been forced to disclose the uniform Defects in its CPUs. Instead, Intel represented that its CPUs were continually improving in speed and performed better than other processors on the market. Plaintiff and the Subclass members acted reasonably in relying on Intel's misrepresentations and omissions, the truth of which they could not have discovered.

824. Intel had a duty to disclose the above facts because members of the public, including Plaintiff and the South Dakota Subclass. Intel's duty to disclose also arose from its: possession of exclusive knowledge regarding the Defects in its CPUs and incomplete

representations about the CPUs, while purposefully withholding material facts from Plaintiff and the South Dakota Subclass that contradicted these representations.

825. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiff and Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues.

826. Intel's violations present a continuing risk to Plaintiff and South Dakota Subclass members as well as to the general public.

827. Plaintiff and South Dakota Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, injunctive relief, and reasonable attorneys' fees and costs.

TENNESSEE SUBCLASS COUNT LV

TENNESSEE CONSUMER PROTECTION ACT,
Tenn. Code Ann. §§ 47-18-101, *et seq.*

828. The Tennessee Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Tennessee Subclass, repeats and re-alleges all previously alleged paragraphs, as if fully alleged herein.

829. Intel is a "person," as defined by Tenn. Code § 47-18-103(13).

830. Plaintiff and Tennessee Subclass members are "consumers," as meant by Tenn. Code § 47-18-103(2).

831. Intel advertised and sold "goods" or "services" in "consumer transaction[s]," as defined by Tenn. Code §§ 47-18-103(7), (18) & (19).

832. Intel advertised, offered, or sold goods or services in Tennessee and engaged in trade or commerce directly or indirectly affecting the people of Tennessee, as defined by Tenn. Code §§ 47-18-103(7), (18) & (19). And Intel's acts or practices affected the conduct of trade or commerce, under Tenn. Code § 47-18-104.

833. Intel intended to mislead Plaintiff and Tennessee Subclass members and induce them to rely on its misrepresentations and omissions.

834. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

835. Had Intel disclosed to Plaintiff and Subclass members material facts, including but not limited to, that in designing its CPUs, it failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks, and was otherwise engaged in deceptive, common business practices, Intel would have been unable to continue in business and it would have been forced to disclose the uniform Defects in its CPUs. Instead, Intel represented that its CPUs were continually improving in speed and performed better than other processors on the market. Plaintiff and the Subclass members acted reasonably in relying on Intel's misrepresentations and omissions, the truth of which they could not have discovered.

836. Intel had a duty to disclose the above facts due to the circumstances of this case. Intel's duty to disclose arose from its: possession of exclusive knowledge regarding the Defects in the CPUs; active concealment of the Defects; and incomplete representations about the Defects in the CPUs, while purposefully withholding material facts from Plaintiff and the Tennessee Subclass that contradicted these representations.

837. Intel's "unfair" acts and practices caused or were likely to cause substantial injury to consumers, which was not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.

838. The injury to consumers was and is substantial because it was non-trivial and non-speculative and involved a monetary injury. The injury to consumers was substantial not only because it inflicted harm on a significant and unprecedented number of consumers, but also because it inflicted a significant amount of harm on each consumer.

839. Consumers could not have reasonably avoided injury because Intel's business acts and practices unreasonably created or took advantage of an obstacle to the free exercise of consumer decision-making. By withholding important information from consumers as described herein, Intel created an asymmetry of information between it and consumers that precluded consumers from taking action to avoid or mitigate injury.

840. Intel's business practices had no countervailing benefit to consumers or to competition.

841. By misrepresenting and omitting material facts, Intel violated the following provisions of Tenn. Code § 47-18-104(b): representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits or quantities that they do not have; representing that goods or services are of a particular standard, quality or grade, if they are of another; advertising goods or services with intent not to sell them as advertised; and representing that a consumer transaction confers or involves rights, remedies or obligations that it does not have or involve. Intel's actions included:

a. Knowingly designing, developing, manufacturing, advertising, and selling CPUs with significant Defects that result in security risks, compromising consumer data, and—if patched—slowing down the CPUs so that consumers did not receive the benefit of their bargain;

b. Marketing and selling Intel CPUs that relied upon speculative execution as a means to achieve higher speeds to compete in the CPU market, while at the same time exposing consumers to side-channel security threats solely to increase profits;

c. Permitting instruction execution in the Intel CPUs without first performing and enforcing the appropriate memory access checks as a means to increase processor speed and, accordingly, putting profits over the safety of consumer data;

d. Failing to take steps to secure the CPU architecture from cache side-channel attacks;

e. Making affirmative public representations about the security of Intel CPUs while, at the same time, not ensuring that safety is a priority in its devices;

f. Making affirmative public representations about the speed of Intel CPUs while knowing that, for those CPUs to offer security for consumer data, they would need to be patched, which would reduce processor speed or leave systems corrupted and still vulnerable; and

g. Concealing and/or failing to disclose material facts, including but not limited to, that in designing its CPUs, it failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks.

842. Intel acted intentionally, knowingly, and maliciously to violate Tennessee's Consumer Protection Act, and recklessly disregarded Plaintiff and Tennessee Subclass members'

rights. Intel's knowledge of the CPUs' security and performance issues put it on notice that the CPUs were not as it advertised.

843. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiff and Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues.

844. Intel's violations present a continuing risk to Plaintiff and Tennessee Subclass members as well as to the general public.

845. Plaintiff and Tennessee Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief, actual damages, treble damages for each willful or knowing violation, attorneys' fees and costs, and any other relief that is necessary and proper.

TEXAS SUBCLASS COUNT LVI

TEXAS DECEPTIVE TRADE PRACTICES—CONSUMER PROTECTION ACT, Texas Bus. & Com. Code §§ 17.41, *et seq.*

846. The Texas Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Texas Subclass, repeats and re-alleges all previously alleged paragraphs, as if fully alleged herein.

847. Intel is a "person," as defined by Tex. Bus. & Com. Code § 17.45(3).

848. Plaintiffs and the Texas Subclass members are "consumers," as defined by Tex. Bus. & Com. Code § 17.45(4).

849. Intel advertised, offered, or sold goods or services in Texas and engaged in trade or commerce directly or indirectly affecting the people of Texas, as defined by Tex. Bus. & Com. Code § 17.45(6).

850. Intel engaged in false, misleading, or deceptive acts and practices, in violation of Tex. Bus. & Com. Code § 17.46(b), including: representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits or quantities that they do not have; representing that goods or services are of a particular standard, quality or grade, if they are of another; and advertising goods or services with intent not to sell them as advertised.

851. Intel intended to mislead Plaintiff and Texas Subclass members and induce them to rely on its misrepresentations and omissions.

852. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

853. Had Intel disclosed to Plaintiff and Subclass members material facts, including but not limited to, that in designing its CPUs, it failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks, and was otherwise engaged in deceptive, common business practices, Intel would have been unable to continue in business and it would have been forced to disclose the uniform Defects in its CPUs. Instead, Intel represented that its CPUs were continually improving in speed and performed better than other processors on the market. Plaintiff and the Subclass members acted reasonably in relying on Intel's misrepresentations and omissions, the truth of which they could not have discovered.

854. Intel had a duty to disclose the above facts due to the circumstances of this case. Intel's duty to disclose arose from its: possession of exclusive knowledge regarding the Defects in its CPUs; and incomplete representations about its CPUs, performance, and security of those CPUs.

855. Intel engaged in unconscionable actions or courses of conduct, in violation of Tex. Bus. & Com. Code Ann. § 17.50(a)(3). Intel engaged in acts or practices which, to consumers' detriment, took advantage of consumers' lack of knowledge, ability, experience, or capacity to a grossly unfair degree.

856. Consumers, including Plaintiffs and Texas Subclass members, lacked knowledge about the above business practices, omissions, and misrepresentations because this information was known exclusively by Intel.

857. Intel intended to take advantage of consumers' lack of knowledge, ability, experience, or capacity to a grossly unfair degree, with reckless disregard of the unfairness that would result. The unfairness resulting from Intel's conduct is glaringly noticeable, flagrant, complete, and unmitigated.

858. Intel acted intentionally, knowingly, and maliciously to violate Texas's Deceptive Trade Practices-Consumer Protection Act, and recklessly disregarded Plaintiff and Texas Subclass members' rights. Intel's knowledge of the CPUs' security and performance issues put it on notice that the CPUs were not as it advertised.

859. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiff and Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues.

860. Intel's violations present a continuing risk to Plaintiffs and Texas Subclass members as well as to the general public.

861. Intel received notice pursuant to Tex. Bus. & Com. Code Ann. § 17.505 concerning its wrongful conduct as alleged herein by Plaintiff and Texas Subclass members. However, sending pre-suit notice pursuant to Tex. Bus. & Com. Code Ann. § 17.505 is an exercise in futility for Plaintiff, as Intel has already been informed of the allegedly unfair and unlawful conduct as described herein as of the date of the first-filed lawsuit, and has yet to offer Class members remedy in accordance with similar consumer protection statute.

862. Intel's actions constitute uniform business practices across the Class, so that all actions Intel took with respect to Class members satisfy the "commonality" prong of Fed. R. Civ. P. 23. No individualized issues concerning Intel's business practices predominate so as to render class treatment inappropriate.

863. Plaintiffs and the Texas Subclass seek all monetary and non-monetary relief allowed by law, including economic damages, damages for mental anguish, treble damages for each act committed intentionally or knowingly, court costs, reasonably and necessary attorneys' fees, injunctive relief, and any other relief which the court deems proper.

UTAH SUBCLASS COUNT LVII

UTAH CONSUMER SALES PRACTICES ACT,
Utah Code §§ 13-11-1, *et seq.*

864. The Utah Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Utah Subclass, repeats and re-alleges all previously alleged paragraphs, as if fully alleged herein.

865. Intel is a "person," as defined by Utah Code § 13-11-1(5).

866. Intel is a "supplier," as defined by Utah Code § 13-11-1(6), because it regularly solicits, engages in, or enforces "consumer transactions," as defined by Utah Code § 13-11-1(2).

867. Intel engaged in deceptive and unconscionable acts and practices in connection with consumer transactions, in violation of Utah Code § 13-11-4 and Utah Code § 13-11-5, as described herein.

868. Intel intended to mislead Plaintiff and Utah Subclass members and induce them to rely on its misrepresentations and omissions.

869. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

870. Had Intel disclosed to Plaintiff and Subclass members material facts, including but not limited to, that in designing its CPUs, it failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks, and was otherwise engaged in deceptive, common business practices, Intel would have been unable to continue in business and it would have been forced to disclose the uniform Defects in its CPUs. Instead, Intel represented that its CPUs were continually improving in speed and performed better than other processors on the market. Plaintiff and the Subclass members acted reasonably in relying on Intel's misrepresentations and omissions, the truth of which they could not have discovered.

871. Intel had a duty to disclose the above facts due to the circumstances of this case. Intel's duty to disclose arose from its: possession of exclusive knowledge regarding the Defects in its CPUs; and incomplete representations about its CPUs, performance, and security.

872. Intel intentionally or knowingly engaged in deceptive acts or practices, violating Utah Code § 13-11-4(2) by: indicating that the subject of a consumer transaction has sponsorship, approval, performance characteristics, accessories, uses, or benefits, if it has not; indicating that the subject of a consumer transaction is of a particular standard, quality, grade, style, or model, if

it is not; indicating that the subject of a consumer transaction has been supplied in accordance with a previous representation, if it has not; indicating that the subject of a consumer transaction will be supplied in greater quantity (e.g., more data security) than the supplier intends.

873. Intel engaged in unconscionable acts and practices that were oppressive and led to unfair surprise, as shown in the setting, purpose, and effect of those acts and practices.

874. In addition, there was an overall imbalance in the obligations and rights imposed by the consumer transactions in question, based on the mores and industry standards of the time and place where they occurred. There is a substantial imbalance between the obligations and rights of consumers, such as Plaintiff and the Utah Subclass, who purchase CPUs based upon the publicly-available information in the marketplace, and Intel, which has exclusive knowledge of any Defects in those devices and software developed to address those Defects.

875. Intel's acts and practices were also procedurally unconscionable because consumers, including Plaintiff and the Utah Subclass, had no practicable option but to purchase CPUs based upon publicly-available information, despite Intel's omissions and misrepresentations.

876. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiff and Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues.

877. Intel's violations present a continuing risk to Plaintiffs and Utah Subclass members as well as to the general public.

878. Plaintiff and Utah Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, statutory damages of $2,000 per violation, amounts necessary to avoid unjust enrichment, under Utah Code §§ 13-11-19, *et seq.*, injunctive relief, and reasonable attorneys' fees and costs.

VERMONT SUBCLASS COUNT LVIII

VERMONT CONSUMER FRAUD ACT,
Vt. Stat. Ann. tit. 9, §§ 2451, *et seq.*

879. The Vermont Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Vermont Subclass, repeats and re-alleges all previously alleged paragraphs, as if fully alleged herein.

880. Plaintiff and Vermont Subclass members are "consumers," as defined by Vt. Stat. Ann. tit. 9, § 2451a(a).

881. Intel's conduct as alleged herein related to "goods" or "services" for personal, family, or household purposes, as defined by Vt. Stat. Ann. tit. 9, § 2451a(b).

882. Intel is a "seller," as defined by Vt. Stat. Ann. tit. 9, § 2451a(c).

883. Intel advertised, offered, or sold goods or services in Vermont and engaged in trade or commerce directly or indirectly affecting the people of Vermont.

884. Intel engaged in unfair and deceptive acts or practices, in violation of Vt. Stat. tit. 9, § 2453(a), as described herein.

885. Intel intended to mislead Plaintiff and Vermont Subclass members and induce them to rely on its misrepresentations and omissions.

886. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

887. Under the circumstances, consumers had a reasonable interpretation of Intel's representations and omissions.

888. Intel had a duty to disclose these facts due to the circumstances of this case. Intel's duty to disclose also from its: possession of exclusive knowledge regarding the Defects in its CPUs; and incomplete representations about the CPUs, performance, and security of same.

889. Intel's acts and practices caused or were likely to cause substantial injury to consumers, which was not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.

890. The injury to consumers was and is substantial because it was non-trivial and non-speculative; and involved a concrete monetary injury. The injury to consumers was substantial not only because it inflicted harm on a significant and unprecedented number of consumers, but also because it inflicted a significant amount of harm on each consumer.

891. Consumers could not have reasonably avoided injury because Intel's business acts and practices unreasonably created or took advantage of an obstacle to the free exercise of consumer decision-making. By withholding important information from consumers, Intel created an asymmetry of information between it and consumers that precluded consumers from taking action to avoid or mitigate injury.

892. Intel's business practices had no countervailing benefit to consumers or to competition.

893. Intel is presumed, as a matter of law under Vt. Stat. Ann. tit. 9, § 2457, to have intentionally violated the Vermont Consumer Protection Act because it failed to sell goods or services in the manner and of the nature advertised or offered.

894. Intel acted intentionally, knowingly, and maliciously to violate Vermont's Consumer Fraud Act, and recklessly disregarded Plaintiff and Vermont Subclass members' rights. Intel's knowledge of the CPUs' security and performance issues put it on notice that the CPUs were not as it advertised.

895. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiff and Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues.

896. Plaintiff and Vermont Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief, restitution, actual damages, disgorgement of profits, treble damages, punitive/exemplary damages, and reasonable attorneys' fees and costs.

VIRGIN ISLANDS SUBCLASS COUNT LIX

VIRGIN ISLANDS CONSUMER FRAUD AND DECEPTIVE BUSINESS PRACTICES ACT V.I. Code tit. 12A, §§ 301, *et seq.*

897. Plaintiffs, on behalf of the Virgin Islands Subclass, repeat and re-allege all previously alleged paragraphs, as if fully alleged herein.

898. Intel is a "person," as defined by V.I. Code tit. 12A, § 303(h).

899. Plaintiff and Virgin Islands Subclass members are "consumers," as defined by V.I. Code tit. 12A, § 303(d).

900. Intel advertised, offered, or sold goods or services in the Virgin Islands and engaged in trade or commerce directly or indirectly affecting the people of the Virgin Islands.

901. Intel engaged in unfair and deceptive acts and practices, in violation of V.I. Code tit. 12A, § 304, as described herein.

902. Intel's acts and practices were "unfair" under V.I. Code tit. 12A, § 304 because they caused or were likely to cause substantial injury to consumers which was not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.

903. The injury to consumers from Intel's conduct was and is substantial because it was non-trivial and non-speculative; and involved a monetary injury. The injury to consumers was substantial not only because it inflicted harm on a significant and unprecedented number of consumers, but also because it inflicted a significant amount of harm on each consumer.

904. Consumers could not have reasonably avoided injury because Intel's business acts and practices unreasonably created or took advantage of an obstacle to the free exercise of consumer decision-making. By withholding important information from consumers, Intel created an asymmetry of information between it and consumers that precluded consumers from taking action to avoid or mitigate injury.

905. Intel's inadequate data security had no countervailing benefit to consumers or to competition.

906. Intel's acts and practices were "deceptive" under V.I. Code tit. 12A, §§ 303 & 304 because Intel made representations or omissions of material facts that had the capacity, tendency or effect of deceiving or misleading consumers, including Plaintiff and Virgin Islands Subclass members.

907. Intel intended to mislead Plaintiff and Virgin Island Subclass members and induce them to rely on its misrepresentations and omissions.

908. Intel's representations and omissions were material because they were likely to unfairly influence or deceive reasonable consumers.

909. Intel had a duty to disclose the above-described facts due to the circumstances of this case. Intel's duty to disclose arose from its: possession of exclusive knowledge regarding the Defects in its CPUs; and incomplete representations about its CPUs, performance, and security.

910. Intel acted intentionally, knowingly, and maliciously to violate the Virgin Island's Consumer Fraud and Deceptive Business Practices Act, and recklessly disregarded Plaintiff and Virgin Islands Subclass members' rights. Intel's knowledge of the CPUs' security and performance issues put it on notice that the CPUs were not as it advertised. Intel intentionally hid this information, callously disregarding the rights of consumers.

911. As a direct and proximate result of Intel's unfair and deceptive acts or practices, Plaintiff and Virgin Islands Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with CPU performance and security issues.

912. Intel's violations present a continuing risk to Plaintiff and Virgin Islands Subclass members as well as to the general public.

913. Plaintiff and Virgin Islands Subclass members seek all monetary and non-monetary relief allowed by law, including compensatory, consequential, treble, punitive, and equitable damages under V.I. Code tit. 12A, § 331, injunctive relief, and reasonable attorneys' fees and costs.

VIRGIN ISLANDS SUBCLASS COUNT LX

VIRGIN ISLANDS CONSUMER PROTECTION LAW, V.I. Code tit. 12A, §§ 101, *et seq.*

914. Plaintiffs, on behalf of the Virgin Islands Subclass, repeat and re-allege all previously alleged paragraphs, as if fully alleged herein.

915. Intel is a "merchant," as defined by V.I. Code tit. 12A, § 102(e).

916. Plaintiff and Virgin Islands Subclass members are "consumers," as defined by V.I. Code tit. 12A, § 102(d).

917. Intel sells and offers for sale "consumer goods" and "consumer services," as defined by V.I. Code tit. 12A, § 102(c).

918. Intel engaged in deceptive acts and practices, in violation of V.I. Code tit. 12A, § 101, as described herein.

919. Intel's acts and practices were "deceptive trade practices" under V.I. Code tit. 12A, § 102(a) because Intel: represented that goods or services have sponsorship, approval, accessories, characteristics, ingredients, uses, benefits, or quantities that they do not have; or that goods or services are of particular standard, quality, grade, style or model, if they are of another; used exaggeration, innuendo or ambiguity as to a material fact or failure to state a material fact if such use deceives or tends to deceive; offered goods or services with intent not to sell them as offered; and stated that a consumer transaction involves consumer rights, remedies or obligations that it does not involve.

920. Intel's acts and practices were also "deceptive" under V.I. Code tit. 12A, § 101 because Intel made representations or omissions of material facts that had the capacity, tendency or effect of deceiving or misleading consumers, including Plaintiff and Virgin Islands Subclass members.

921. Intel intended to mislead Plaintiff and Virgin Islands Subclass members and induce them to rely on its misrepresentations and omissions.

922. Intel representations and omissions were material because they were likely to deceive reasonable consumers.

923. Intel had a duty to disclose the above-described facts due to the circumstances of this case, as alleged herein.

924. Intel acted intentionally, knowingly, and maliciously to violate the Virgin Island's Consumer Protection Law, and recklessly disregarded Plaintiff and Virgin Island Subclass members' rights. Intel's knowledge of the CPUs' security and performance issues put it on notice that the CPUs were not as it advertised.

925. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiff and Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues.

926. Intel's violations present a continuing risk to Plaintiff and Virgin Islands Subclass members as well as to the general public.

927. Plaintiff and Virgin Islands Subclass members seek all monetary and non-monetary relief allowed by law, including declaratory relief; injunctive relief, the greater of actual damages or $500 per violation, compensatory, consequential, treble, and punitive damages; disgorgement, and reasonable attorneys' fees and costs.

VIRGINIA SUBCLASS COUNT LXI

VIRGINIA CONSUMER PROTECTION ACT,
Va. Code Ann. §§ 59.1-196, *et seq.*

928. The Virginia Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Virginia Subclass, repeats and re-alleges all previously alleged paragraphs, as if fully alleged herein.

929. The Virginia Consumer Protection Act prohibits "[u]sing any . . . deception, fraud, false pretense, false promise, or misrepresentation in connection with a consumer transaction." Va. Code Ann. § 59.1-200(14).

930. Intel is a "person" as defined by Va. Code Ann. § 59.1-198.

931. Intel is a "supplier," as defined by Va. Code Ann. § 59.1-198.

932. Intel engaged in the complained-of conduct in connection with "consumer transactions" with regard to "goods" and "services," as defined by Va. Code Ann. § 59.1-198. Intel advertised, offered, or sold goods or services used primarily for personal, family or household purposes.

933. Intel engaged in deceptive acts and practices by using deception, fraud, false pretense, false promise, and misrepresentation in connection with consumer transactions, described herein.

934. Intel intended to mislead Plaintiff and Virginia Subclass members and induce them to rely on its misrepresentations and omissions.

935. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

936. Had Intel disclosed to Plaintiff and Subclass members material facts, including but not limited to, that in designing its CPUs, it failed to take measures to protect confidential

information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks, and was otherwise engaged in deceptive, common business practices, Intel would have been unable to continue in business and it would have been forced to disclose the uniform Defects in its CPUs. Instead, Intel represented that its CPUs were continually improving in speed and performed better than other processors on the market. Plaintiff and the Subclass members acted reasonably in relying on Intel's misrepresentations and omissions, the truth of which they could not have discovered.

937. Intel had a duty to disclose these facts due to the circumstances of this case due to its exclusive knowledge of the Defects, concealment of those Defects, and incomplete representations regarding its CPUs.

938. The above-described deceptive acts and practices also violated the following provisions of VA Code § 59.1-200(A): misrepresenting that goods or services have certain quantities, characteristics, ingredients, uses, or benefits; misrepresenting that goods or services are of a particular standard, quality, grade, style, or model; and advertising goods or services with intent not to sell them as advertised, or with intent not to sell them upon the terms advertised.

939. Intel acted intentionally, knowingly, and maliciously to violate Virginia's Consumer Protection Act, and recklessly disregarded Plaintiff and Virginia Subclass members' rights. Intel's knowledge of the CPUs' security and performance issues put it on notice that the CPUs were not as it advertised. An award of punitive damages would serve to punish Intel for its wrongdoing and warn or deter others from engaging in similar conduct.

940. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiff and Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of

their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues.

941. Intel's violations present a continuing risk to Plaintiffs and Virginia Subclass members as well as to the general public.

942. Plaintiff and Virginia Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages; statutory damages in the amount of $1,000 per violation if the conduct is found to be willful or, in the alternative, $500 per violation, restitution, injunctive relief, punitive damages, and attorneys' fees and costs.

WASHINGTON SUBCLASS COUNT LXII

WASHINGTON CONSUMER PROTECTION ACT,
Wash. Rev. Code Ann. §§ 19.86.020, *et seq.*

943. The Washington Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Washington Subclass, repeats and re-alleges all previously alleged paragraphs, as if fully alleged herein.

944. Intel is a "person," as defined by Wash. Rev. Code Ann. § 19.86.010(1).

945. Intel advertised, offered, or sold goods or services in Washington and engaged in trade or commerce directly or indirectly affecting the people of Washington, as defined by Wash. Rev. Code Ann. § 19.86.010 (2).

946. Intel engaged in unfair or deceptive acts or practices in the conduct of trade or commerce, in violation of Wash. Rev. Code Ann. § 19.86.020, as described herein.

947. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

948. Intel acted intentionally, knowingly, and maliciously to violate Washington's Consumer Protection Act, and recklessly disregarded Plaintiff and Washington Subclass members'

rights. Intel's knowledge of the CPUs' security and performance issues put it on notice that the CPUs were not as it advertised.

949. Intel's conduct is injurious to the public interest because it violates Wash. Rev. Code Ann. § 19.86.020, violates a statute that contains a specific legislation declaration of public interest impact, and/or injured persons and had and has the capacity to injure persons. Further, its conduct affected the public interest, including the at least hundreds of thousands of Washingtonians affected by Intel's deceptive business practices.

950. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiff and Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues

951. Plaintiff and Washington Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, treble damages, injunctive relief, civil penalties, and attorneys' fees and costs.

WEST VIRGINIA SUBCLASS COUNT LXIII

WEST VIRGINIA CONSUMER CREDIT AND PROTECTION ACT,
W. Va. Code §§ 46A-6-101, *et seq.*

952. The West Virginia Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the West Virginia Subclass, repeats and re-alleges all previously alleged paragraphs, as if fully alleged herein.

953. Plaintiff and West Virginia Subclass members are "consumers," as defined by W. Va. Code § 46A-6-102(2).

954. Intel engaged in "consumer transactions," as defined by W. Va. Code § 46A-6-102(2).

955. Intel advertised, offered, or sold goods or services in West Virginia and engaged in trade or commerce directly or indirectly affecting the people of West Virginia, as defined by W. Va. Code § 46A-6-102(6).

956. Intel received notice pursuant to W. Va. Code § 46A-6-106(c) concerning its wrongful conduct as alleged herein by Plaintiff and West Virginia Subclass members. However, sending pre-suit notice pursuant to W. Va. Code § 46A-6-106(c) is an exercise in futility for Plaintiff, because, despite being on knowledge of the deceptive acts and practices complained of herein in this lawsuit as of the date of the first-filed lawsuit, Intel has not cured its unfair and deceptive acts and practices.

957. Intel engaged in unfair and deceptive business acts and practices in the conduct of trade or commerce, in violation of W. Va. Code § 46A-6-104, as described herein.

958. Intel's unfair and deceptive acts and practices also violated W. Va. Code § 46A-6-102(7), including: representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits or quantities that they do not have; representing that goods or services are of a particular standard, quality or grade, or that goods are of a particular style or model if they are of another; advertising goods or services with intent not to sell them as advertised; engaging in any other conduct which similarly creates a likelihood of confusion or of misunderstanding; using deception, fraud, false pretense, false promise or misrepresentation, or the concealment, suppression or omission of any material fact with intent that others rely upon such concealment, suppression or omission, in connection with the sale or advertisement of goods or services, whether or not any person has in fact been misled, deceived or damaged thereby; and advertising,

displaying, publishing, distributing, or causing to be advertised, displayed, published, or distributed in any manner, statements and representations with regard to the sale of goods, which are false, misleading or deceptive or which omit to state material information which is necessary to make the statements therein not false, misleading or deceptive.

959. Intel's unfair and deceptive acts and practices were unreasonable when weighed against the need to develop or preserve business, and were injurious to the public interest, under W. Va. Code § 46A-6-101.

960. Intel's acts and practices were additionally "unfair" under W. Va. Code § 46A-6-104 because they caused or were likely to cause substantial injury to consumers which was not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.

961. The injury to consumers from Intel's conduct was and is substantial because it was non-trivial and non-speculative; and involved a monetary injury. The injury to consumers was substantial not only because it inflicted harm on a significant and unprecedented number of consumers, but also because it inflicted a significant amount of harm on each consumer.

962. Consumers could not have reasonably avoided injury because Intel's business acts and practices unreasonably created or took advantage of an obstacle to the free exercise of consumer decision-making. By withholding important information from consumers, Intel created an asymmetry of information between it and consumers that precluded consumers from taking action to avoid or mitigate injury.

963. Intel's business practices had no countervailing benefit to consumers or to competition.

964. Intel's acts and practices were additionally "deceptive" under W. Va. Code § 46A-6-104 because Intel made representations or omissions of material facts that misled or were likely to mislead reasonable consumers, including Plaintiff and West Virginia Subclass members.

965. Intel intended to mislead Plaintiff and West Virginia Subclass members and induce them to rely on its misrepresentations and omissions.

966. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

967. Had Intel disclosed to Plaintiff and Subclass members material facts, including but not limited to, that in designing its CPUs, it failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks, and was otherwise engaged in deceptive, common business practices, Intel would have been unable to continue in business and it would have been forced to disclose the uniform Defects in its CPUs. Instead, Intel represented that its CPUs were continually improving in speed and performed better than other processors on the market. Plaintiff and the Subclass members acted reasonably in relying on Intel's misrepresentations and omissions, the truth of which they could not have discovered.

968. Intel had a duty to disclose the above-described facts due to the circumstances of this case because of its exclusive knowledge of the CPUs' Defects, its concealment of same, and its incomplete representations about its CPUs.

969. Intel's omissions were legally presumed to be equivalent to active misrepresentations because Intel intentionally prevented Plaintiff and West Virginia Subclass members from discovering the truth regarding Intel's CPU Defects.

970. Intel acted intentionally, knowingly, and maliciously to violate West Virginia's Consumer Credit and Protection Act, and recklessly disregarded Plaintiff and West Virginia Subclass members' rights. Intel's unfair and deceptive acts and practices were likely to cause serious harm, and Intel knew that its deceptive acts would cause harm based upon its business practices and exclusive knowledge of the omissions and misrepresentations herein.

971. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiff and Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues.

972. Intel's violations present a continuing risk to Plaintiff and West Virginia Subclass members as well as to the general public.

973. Plaintiff and West Virginia Subclass members seek all monetary and non-monetary relief allowed by law, including the greater of actual damages or $200 per violation under W. Va. Code § 46A-6-106(a), restitution, injunctive and other equitable relief, punitive damages, and reasonable attorneys' fees and costs.

<u>WISCONSIN SUBCLASS COUNT LXIV</u>

WISCONSIN DECEPTIVE TRADE PRACTICES ACT,
Wis. Stat. §§ 100.18, *et seq.*

974. The Wisconsin Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Wisconsin Subclass, repeats and re-alleges all previously alleged paragraphs, as if fully alleged herein.

975. Intel is a "person, firm, corporation or association," as defined by Wis. Stat. § 100.18(1).

976. Plaintiff and Wisconsin Subclass members are members of "the public," as defined by Wis. Stat. § 100.18(1).

977. With intent to sell, distribute, or increase consumption of merchandise, services, or anything else offered by Intel to members of the public for sale, use, or distribution, Intel made, published, circulated, placed before the public or caused (directly or indirectly) to be made, published, circulated, or placed before the public in Wisconsin advertisements, announcements, statements, and representations to the public which contained assertions, representations, or statements of fact which are untrue, deceptive, and/or misleading, in violation of Wis. Stat. § 100.18(1).

978. Intel also engaged in the above-described conduct as part of a plan or scheme, the purpose or effect of which was to sell, purchase, or use merchandise or services not as advertised, in violation of Wis. Stat. § 100.18(9).

979. Intel intended to mislead Plaintiff and Wisconsin Subclass members and induce them to rely on its misrepresentations and omissions.

980. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

981. Intel's had a duty to disclose the above-described facts due to the circumstances of this case including its exclusive knowledge of the CPU Defects, its concealment regarding same, and its incomplete representations regarding its CPUs.

982. Intel's failure to disclose the above-described facts is the same as actively representing that those facts do not exist.

983. Intel acted intentionally, knowingly, and maliciously to violate the Wisconsin Deceptive Trade Practices Act, and recklessly disregarded Plaintiff and Wisconsin Subclass

members' rights. Intel's knowledge of the CPUs' performance and security issues put it on notice that the CPUs were not as it advertised.

984. As a direct and proximate result of Intel's deceptive acts or practices, Plaintiff and Wisconsin Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with CPU performance and security issues.

985. Intel had an ongoing duty to all Intel customers to refrain from deceptive acts, practices, plans, and schemes under Wis. Stat. § 100.18.

986. Plaintiff and Wisconsin Subclass members seek all monetary and non-monetary relief allowed by law, including damages, reasonable attorneys' fees, and costs under Wis. Stat. § 100.18(11)(b)(2), injunctive relief, and punitive damages.

WYOMING SUBCLASS COUNT LXV

WYOMING CONSUMER PROTECTION ACT,
Wyo. Stat. Ann. §§ 40-12-101, *et seq.*

987. The Wyoming Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Wyoming Subclass, repeats and re-alleges all previously alleged paragraphs, as if fully alleged herein.

988. Intel is a "person" as defined by Wyo. Stat. Ann. § 42-12-102(i).

989. Plaintiff and Wyoming Subclass members engaged in "consumer transactions" as defined by Wyo. Stat. Ann. § 40-12-102(ii).

990. Intel is engaged in an "uncured unlawful deceptive trade practice" in accordance with Wyo. Stat. Ann. § 40-12-105 in that it had actual notice of its deceptive acts and practices when the first-filed case in this multidistrict litigation was filed; however, it has not offered to

adjust or modified the consumer transactions at issue in this case, nor has it offered to rescind the consumer transactions. Accordingly, although notice was sent to Intel pursuant to Wyo. Stat. Ann. § 40-12-109, notice is an exercise in futility for Plaintiff.

991. Intel advertised, offered, or sold goods or services in Wyoming, and engaged in trade or commerce directly or indirectly affecting the people of Wyoming.

992. Intel engaged in deceptive acts and practices in the conduct of trade or commerce, in violation of the Wyoming Consumer Protection Act, Wyo. Stat. Ann. §§ 40-12-101, *et seq*., including: representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or qualities that they do not have; representing that goods or services are of a particular standard, quality, or grade, or that goods are of a particular style or model, if they are of another; and engaging in any other unconscionable, false, misleading, or deceptive act or practice in the conduct of trade or commerce.

993. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

994. Intel intended to mislead Plaintiff and Wyoming Subclass members and induce them to rely on its misrepresentations and omissions.

995. Had Intel disclosed to Plaintiff and Subclass members material facts, including but not limited to, that in designing its CPUs, it failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks, and was otherwise engaged in deceptive, common business practices, Intel would have been unable to continue in business and it would have been forced to disclose the uniform Defects in its CPUs. Instead, Intel represented that its CPUs were continually improving in speed and performed better than other processors on the market. Plaintiff and the Subclass members

acted reasonably in relying on Intel's misrepresentations and omissions, the truth of which they could not have discovered.

996. Intel acted intentionally, knowingly, and maliciously to violate the Wyoming Consumer Protection Act, and recklessly disregarded Plaintiff and Wyoming Subclass members' rights. Intel's knowledge of the CPUs' security and performance issues put it on notice that the CPUs were not as it advertised.

997. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiff and Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues.

998. Intel's deceptive acts and practices caused substantial injury to Plaintiff and Wyoming Subclass members, which they could not reasonably avoid, and which outweighed any benefits to consumers or to competition.

999. Plaintiff and the Wyoming Subclass seek all monetary and non-monetary relief allowed by law, actual damages, injunctive relief, attorneys' fees, costs, and any other relief that is just and proper.

REQUEST FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all other Class members, respectfully request that the Court enter an Order:

A. Declaring that this action is a proper class action, certifying the Class and/or Subclasses as requested herein, designating Plaintiffs as Class Representatives, and appointing Plaintiffs' attorneys as Class Counsel;

B. Enjoining Intel from continuing the unfair business practices alleged in this Complaint;

C. Ordering Intel to pay actual and statutory damages (including punitive damages) and restitution to Plaintiffs and the other Class members, as allowable by law;

D. Ordering Intel to pay both pre- and post-judgment interest on any amounts awarded;

E. Ordering Intel to pay attorneys' fees and costs of suit; and

F. Ordering such other and further relief as may be just and proper.

JURY DEMAND

Plaintiffs hereby demand a trial by jury on all issues so triable.

DATED this 24th day of August, 2018.

STOLL STOLL BERNE LOKTING
& SHLACHTER P.C.

By: s/Jennifer S. Wagner
Steve D. Larson, OSB No. 863540
Jennifer S. Wagner, OSB No. 024470

209 SW Oak Street, Suite 500
Portland, Oregon 97204
Telephone: (503) 227-1600
Email: slarson@stollberne.com
jwagner@stollberne.com

Interim Plaintiffs' Liaison Counsel

Christopher A. Seeger (*pro hac vice*)
SEEGER WEISS LLP
55 Challenger Road
Ridgefield Park, NJ 07660
Telephone: (212) 584-0700
Email: cseeger@seegerweiss.com

Rosemary M. Rivas (*pro hac vice*)
LEVI & KORSINSKY LLP
44 Montgomery Street, Suite 650
San Francisco, CA 94104
Telephone: (415) 291-2420
Email: rrivas@zlk.com

Interim Co-Lead Plaintiffs' Counsel

Gayle M. Blatt (*pro hac vice*)
CASEY GERRY SCHENK FRANCAVILLA
BLATT & PENFIELD LLP
110 Laurel Street
San Diego, CA 92101
Telephone: (619) 238-1811
Email: gmb@cglaw.com

Stuart A. Davidson (*pro hac vice*)
ROBBINS GELLER RUDMAN & DOWD
LLP
120 East Palmetto Park Road, Suite 500 Boca
Raton, FL 33432
Telephone: (561) 750-3000
Email: sdavidson@rgrdlaw.com

Melissa R. Emert (*pro hac vice*)
STULL, STULL, & BRODY
6 East 45th Street
New York City, NY 10017
Telephone: (212) 687-7230
Email: memert@ssbny.com

Richard M. Hagstrom (*pro hac vice*)
HELLMUTH & JOHNSON PLLC
8050 West 78th Street
Edina, MN 55439
Telephone: (952) 941-4005
Email: rhagstrom@hjlawfirm.com

Jennifer L. Joost (*pro hac vice*)
KESSLER TOPAZ MELTZER & CHECK
LLP
One Sansome Street, Suite 1850
San Francisco, CA 94104
Telephone: (415) 400-3000
Email: jjoost@ktmc.com

Adam J. Levitt (*pro hac vice*)
DICELLO LEVITT & CASEY LLC
Ten North Dearborn Street, Eleventh Floor
Chicago, IL 60602
Telephone: (312) 214-7900
Email: alevitt@dlcfirm.com

Charles E. Schaffer (*pro hac vice*)
LEVIN SEDRAN & BERMAN LLP
510 Walnut Street, Suite 500
Philadelphia, PA 19106
Telephone: (215) 592-1500
Email: cschaffer@lfsblaw.com

Interim Plaintiffs' Steering Committee